CONFERENCE PROCEEDINGS

Health Records: Social Needs and Personal Privacy

Washington, DC
February 11-12, 1993
Omni Shoreham Hotel

SPONSORED BY THE

Task Force on Privacy, Office of the
Assistant Secretary for Planning and Evaluation
and the Agency for Health Care Policy and Research (HHS)

4441

CONFERENCE PROCEEDINGS

Health Records: Social Needs and Personal Privacy

Washington, DC
February 11-12, 1993
Omni Shoreham Hotel

SPONSORED BY THE

Task Force on Privacy, Office of the
Assistant Secretary for Planning and Evaluation
and the Agency for Health Care Policy and Research (HHS)

For sale by the U.S. Government Printing Office
Superintendent of Documents, Mail Stop: SSOP, Washington. DC 20402-9328
ISBN 0-16-043087-9

Office of the Assistant Secretary for Planning and Evaluation
David Ellwood, Ph.D., Assistant Secretary for Planning & Evaluation

Public Health Service
Philip R. Lee, M.D., Assistant Secretary for Health

Office of Program Systems
Gerald Britten, Deputy Assistant Secretary for Program Systems

Agency for Health Care Policy and Research
J. Jarret Clinton, M.D., M.P.H., Administrator

Acknowledgments

Kunitz and Associates, Inc., under contract (I-II-IS-100-91-0036) to the Office of the Assistant Secretary for Planning and Evaluation, Department of Health and Human Services, provided support to the Task Force. We thank Rene Kozloff, Ph.D., the project manager, and Michele Gargano, M.Sc., who had primary responsibility for this effort. Thanks also go to members of the Task Force, who contributed their energy and expertise to the design and implementation of the conference, and specifically to Joan Turek-Brezina, Ph.D., Harvey Schwartz, Ph.D., John Fanning, LL.B., and Lois Alexander, J.D., of the Department of Health and Human Services; and Patricia Faley of the U.S. Office of Consumer Affairs, who comprised the Executive Committee for the conference.

Statement of the Sponsors

The conference, *Health Records: Social Needs and Personal Privacy*, jointly sponsored by the Office of the Assistant Secretary for Planning and Evaluation and the Agency for Health Care Policy and Research, explored the most appropriate and effective methods to maintain a balance between the privacy of health records and the legitimate needs for information while facilitating the development of the electronic health system and health records. The conference speakers and participants examined the uses of health information, the effect of health information upon individual rights, and the best means for society to strike the balance between the privacy of health records and the need for data in the future.

This conference was held as part of the work being undertaken by the Task Force on Privacy which was established by the Assistant Secretary for Planning and Evaluation in response to a request by the U.S. Office for Consumer Affairs to the Secretary of the Department of Health and Human Services, Louis W. Sullivan, in response to the growing concern about the privacy of health records. The Task Force was initially charged with examining the use of health records that are personally identifiable while recognizing needs for information in the public and private sectors. In conjunction with this work and in response to emerging health care initiatives, the Task Force refocused its efforts on moving toward electronic records within the context of health care reform efforts.

Prior to the conference, the Task Force met with and solicited testimony from over 30 organizations representing the provider community, public health sector, academia, private industry, and privacy advocacy groups. The individuals representing these organizations and sectors provided the Task Force with first-hand experience and knowledge and informed viewpoints. From these unique perspectives, the speakers identified current problems in protecting privacy as well as potential areas of danger in the future as a result of new technology and increased automation in the health care industry; described steps, procedures, and technologies currently being utilized to protect privacy and data; and informed the Task Force about the special needs of the individual as a patient, a provider of data, and a research subject. These sessions gave the representatives an opportunity to make recommendations about future directions and issues for the Task Force to pursue; privacy provisions in future legislation; as well as the most appropriate and effective means to protect privacy, data, and the individual. They also helped in developing the agenda for this conference.

The information gathered through the conference and the presentations to the Task Force have been important in the formation of the knowledge base from which the Task Force is formulating privacy considerations and completing its intended mission. The Task Force anticipates completing all work by January 1994.

Joan Turek-Brezina, Ph.D.
Chairperson, Task Force on the Privacy of Private-Sector Health Records

Harvey A. Schwartz, Ph.D.
Co-Sponsor **of the Conference, Agency for Health Care Policy an&Research**

Foreword

This volume features presentations from a conference on the most appropriate and effective methods to maintain a balance between the privacy of health records and the legitimate needs for information while facilitating the development of the electronic health system and health records. The conference was jointly sponsored by the Office of the Assistant Secretary for Planning and Evaluation (ASPE) and the Agency for Health Care Policy and Research (AHCPR) in February 1993 in Washington, D.C.

The papers that were presented examined the practical uses of health information, the effect of health information upon individual rights, privacy and confidentiality guidelines and policies, and safeguards in the protection of electronic health care information. Problems in accessing and using such information, as well as suggestions for overcoming these problems, are discussed.

We trust that the guidance offered within these pages will prove useful to consumers, patients, providers of health care, researchers, government officials, health insurers, direct marketers, credit bureaus, employers, and those who design and maintain health-related data systems.

HHS Task Force on the Privacy of Private-Sector Health Records*

Joan Turek-Brezina, Chairperson
Office of the Assistant Secretary for Planning and Evaluation

Lois Alexander
Social *Security Administration*

A. Prentice Barnes
Office of the Asslstant Secretary for Management and Budget

Johanna Bonnelycke
Office of the Assistant Secretary for Health, PHS

Susan Callahan
Office of the General Counsel

Thomas Donnelly
Office of the Assistant Secretary for Public Affairs

Willie Etheridge
Administration for Children, Youth, and Families

John P. Fanning
Office of Health Planning and Evaluation, PHS

Richard Friedman
Office of the General Counsel

W. Keith Lively
Office of the Assistant Secretary for Planning and Evaluation

Stanley Rosenfeld
Health Care Financing Administration

Harvey A. Schwartz
Agency *for* Health *Care* Policy and Research, PHS

Patricia Faley, Ex Officio
United States Office of Consumer Affairs

• As of February 12, 1993. For an updated list of Task Force members, see Appendix A.

Contents

Welcome

Joan Turek-Brezina, Ph.D.
Chairperson
Task Force on the Privacy of Private-Sector Health Records

Welcome to our conference, *Health Records: Social Needs and Personal Privacy,* being conducted by the Privacy Task Force under the joint sponsorship of the Office of the Assistant Secretary for Planning and Evaluation and the Agency for Health Policy and Research.

Before proceeding with the substance of the conference, I have two brief announcements:

- All presentations will be tape recorded. Please do not make tape recordings, since the proceeding will be available after the meeting.
- Media representatives are present in the audience. We extend them our welcome and ask that they obtain speakers' permission before quoting them by name.

This conference is one of the activities of the Task Force in seeking the perspective of a broad audience regarding the issues it has been asked to address.

The Task Force was established in 1990 with membership drawn from the major operating units of the Department of Health and Human Services. I will introduce these Task Force members, who can be identified by the blue ribbons attached to their name tags, at today's luncheon.

The Task Force was initially charged with

- Examining the extent of the problems with the use of personally identifiable medical and other health-related records in the private sector;
- Identifying health information needs in the public and private sector;
- Reviewing the current laws and practices of privacy of private sector health records; and
- Recommending steps that the federal government could, if problems were identified, appropriately pursue to protect nonfederal record systems.

Since the Task Force's founding, emerging events have refocused its mission to focus on efforts to develop electronic health care information systems in the context of health care reform. I will leave it to our next two speakers, in their opening remarks, to discuss future directions. ◆◆

Conference Overview

Gerald Britten
Deputy Assistant Secretary for Program Services
Department of Health and Human Services

On behalf of Secretary Shalala, I welcome you to this conference. Not since the late 1970s when the Privacy Protection Study Commission examined all types of records has there been such strong interest in privacy issues.

This renewed interest, focusing on health records, springs from both health care reform efforts and the ongoing revolution in information technology.

The timing of this conference is superb. You are addressing a key issue: how to balance the much greater use of and access to automated health records with privacy concerns.

As you know, President Clinton has set a goal of submitting a health care reform package to Congress within 100 days of his inauguration. Many experts are at work almost round the clock on this health care reform package. Clearly, one component will be reducing administrative costs in the health care systems-estimated in the multi-billion dollar range. A key element in this strategy is the expanded use of automated health care information systems.

Automated Systems

Even without health care reform, the development of such systems is becoming a reality. Development is viewed as central to reducing paperwork burdens and costs and improving the quality and coordination of patient care.

- Automating insurance claims processes can eliminate enormous paperwork burdens from patients, providers, and insurers, and provide a more efficient and timely reimbursement system.
- Automating patients' health care records can result in quality improvements that will add value to each health care dollar spent. Hospitals are finding that automation can improve the quality and timeliness of care they deliver. In our mobile society patients' records need to be transferred faster as patients move from provider to provider.

The systemic changes envisioned under health care reform will increase the need for micro-level, standard information permitting providers, consumers, and other players to have high-quality information on health cam, including price and outcome information.

While particular groups vary in their specific vision, those focusing on development of automated health care systems (such as the Computer-Based Patient Record Institute, Medical Record Institute, and American National Standards Institute) see a system of several parts:

- A comprehensive longitudinal computer-based patient record containing all clinical, financial, and research data;
- A national electronic network of accessing this health record for a variety of purposes such as primary care, insurance payment, peer review, cost containment, public health, and research purposes;
- Use of a smart card for purposes ranging from providing health insurance coverage information to providing a conception-to-death record of health care;
- Use of unique patient-specific identifiers nationally and, perhaps, worldwide.

Privacy Concerns

Major privacy issues must be addressed as all this goes on. First, at a macro level, privacy generally is a growing concern, especially since we have experienced increasingly rapid growth in the amount of personal information collected by and shared among public and private organizations.

A number of polls show that concern for personal privacy is greater in the '90s.' A 1992 poll found that a majority of the American public feels that protection of consumer information will get worse by 2000.[2] While acknowledging

the benefits computers have brought to society and their own lives, survey respondents also expressed concern about the dangers of present computer uses to personal privacy.

Second, computerization facilitates use of information and alters the risks associated with that use. Data, once available only on paper in an office file, are now accessible electronically from a distance. Consequently, they are more accessible to many more people than are paper files. The range of uses may increase in ways not initially expected, and new data uses may be detrimental to personal privacy.

Third, in the health care arena particularly, changes have contributed to privacy concerns:

- More and more people review medical records in an effort to provide health care and ancillary services. For example, when an individual is hospitalized today, the patient's medical information may be reviewed by attending physicians (including medical students at teaching hospitals), nurses, medical-record personnel, laboratory technicians, billing personnel, insurance-claims processors, medical-records review company staff, medical researchers, and computer specialists designing or testing a computer system or program. If a lawsuit is involved, attorneys will be given copies of the medical record. If the patient needs to apply for a loan to pay for the part of the bill not covered by .a third-party **payor,** the bank will be given at least some health information. Simply put, many people need to know certain information to help a particular individual.
- More organizations are sharing computerized health information. Researchers share data with other researchers to obviate resurveying the same population. National databases maintain information about people's health status. Insurance companies consult this information when deciding whether to extend coverage to an applicant. Employers consult similar databases, as well as databases containing information on workmen's compensation claims, when deciding to hire job applicants.
- New confidentiality problems are **presented** by HIV infection and genetic screening, which can determine an individual's predisposition to certain serious illnesses. These issues are in addition to the continuing privacy problems posed by drug and alcohol abuse and mental illness, which were among the most sensitive issues in the past. All of these are conditions that can affect a person's access to insurance, employment, or other opportunities.
- Researchers need growing access to information to address policy and operational issues concerning health care.
- New kinds of health records continue to emerge. Increasing numbers of pharmacies and supermarket chains are maintaining computerized records on personal drug use. Efforts are under way to develop further information on the public's consumption patterns for direct-mail marketing including collecting information on the types of over-the-counter drugs and medical devices consumers purchase. Medical providers are also increasingly accepting credit card payment from their patients, thereby fostering a body of health data in VISA, Mastercard, and other credit-card systems.

Yet despite this, the record on privacy to date appears generally to be good.

Developing a Balance

Our challenge-indeed, your challenge-is to help develop an appropriate balance between access and privacy. How can the various entities and people involved in health care delivery and policy have access to the information needed for informed decisionmaking while still having confidence that private information is protected from unnecessary disclosure?

-How can we ensure the reliability of information? How can we effectively control unwarranted incursions into information of a very private nature? And who should be the arbiter?

The greatest impediment to development of electronic data systems may be concern for individual privacy However, given the great benefits that can be realized **from** automation, these concerns should not create a barrier to development of such systems. They should instead direct our attention toward establishing an appropriate balance between social needs and personal privacy-the central issue of this conference.

Automation of health care records, if done appropriately, can both strengthen patient privacy and confidentiality and assure **that information** is available to improve the quality and efficiency of health care services. Otherwise,

needed improvements in the efficiency and effectiveness of health care will not be fully realized, and those who supply information can be harmed by inappropriate disclosures.

The issues you will be addressing over the next two days are critically important. I wish you well; we look forward to the results of your endeavors.

Endnotes

1. Equifax Report on Consumers in the Information Age. 1990. National opinion survey conducted by Louis Harris & Associates and Dr. Alan F. Westin, Columbia University
2. Harris-Equifax Consumer Privacy Survey. 1592. Conducted by Louis Harris & Associates in association with Dr. Alan F. Westin, Columbia University. This is the second annual update to the 1990 report. ◆◆

Opening Remarks

J. Jarrett Clinton, M.D., M.P.H.
Administrator
Agency for Health Care Policy and Research

I join with my colleagues to welcome you to this DHHS conference. My assignment is to say a few words about the theme of the conference, provide some background about the Agency for Health Care Policy and Research, and outline what you can do for us.

Balancing Privacy and Society's Needs

The theme is balancing privacy and society's needs. privacy has been a fundamental value in this country since its founding. But the right to privacy is increasingly challenged as society grapples with the need to balance individual rights to privacy with information needs of the society at large. An easy analogy is property rights.

I am fortunate to own a home in the Virginia suburbs. Recently, I recognized that the property I am paying for had been "invaded" by the state to build a road. The concept of eminent domain applies here. I had to give up some of my property for a road available not only for my benefit but for general public use. But we cannot easily see a direct connection between giving up some of our privacy for our personal benefit and for the greater benefit of our society.

We are now closely examining the notion that we could produce better information for clinical care, create "clinical practice guidelines," and assist consumers to make the health care marketplace work more appropriately and more efficiently by providing better information about the quality of care delivered by their provider and the health cam system. But this can only be achieved if each of us is willing to give up a little bit of privacy.

Yielding some personal privacy to achieve a larger goal is not a new concept, but we sense a new urgency as a result of health care reform efforts. Never before has the urgency to look at integrated services and health records been greater. How much privacy is invaded when a complete clinical record moves through what we describe as comprehensive and integrated systems?

For example, HIV patients require a great number of services from many providers-not just in the narrow health system, but also in the broader social services and housing sectors. If this information is in a written record or computer disk, should it be available to the researchers? These are the issues that we struggle to resolve.

Improving Consumer Understanding

The health care system does not work well in the marketplace, and much of the health care reform initiative is looking at ways the system might be improved. One way is to improve the consumer's understanding of what is occurring. Which practitioners provide better care? What are the outcomes of Hospital A versus Hospital B? And how much are the premiums for the policy that you want to buy? What are the benefits of the health insurance that your employer buys, and how much of the insurance costs affects your own pay? These are questions that we are trying to answer.

But we cannot provide that information unless we have the aggregate information extracted from your medical record, my medical record, and the results of care from thousands of individuals. So the theme is right. How do we balance the nation's great concern about the cost and quality of medical care with this deeply held value of privacy?

The Agency for Health Care Policy and Research (AHCPR) was created by Congress in 1989 to succeed the National Center for Health Services Research, which had been established 20 years earlier within the Public Health Service. We are a proactive agency concerned not only with cost, financing, and access to health care but also the effectiveness of health care. The agency's charge from Congress is to look at the research on the typical community, the typical patient, and the typical doctor, and determine what seems to work best. This kind of information is not available from highly controlled clinical trials.

Accounting for Practice Variations

We want to know what happens when the average internist sees the average patient, for example, in Dodge City, Kansas. Does the same outcome occur when the internist and patient are in San Francisco or Birmingham, Alabama? If not, how do we account for these variations in practice? If it does not make any difference, then the issues are not significant. However, in some instances, the variations in practice are considerable but the outcomes seem about the same. In other instances, variations are great, unexplainable, and associated with considerably different outcomes.

Plenty of evidence indicates that medical practice varies enormously; so do the outcomes concerning the cost, the functional capacity of the individual, and the physiological markers traditionally used to measure the results of medical care.

The National Library of Medicine accepts a thousand new articles every day. The public expects clinicians to learn all that is in these articles, to interpret complicated scientific presentations-in essence, to put them in a working context useful to Dodge City. The AHCPR-supported, practice guideline work synthesizes this information for clinicians and helps consumers ask questions to discuss treatment options. If you are in a car wreck and are unconscious, or if you have a myocardial infarction, you are not likely to be in any condition to talk about these things. But if you are considering a hysterectomy, the management of a breast lump, or the management of back pain, you should take the opportunity to talk about the options available to you. Therein lies our interest in informing consumers about their medical care and informing the general public about the quality of medical care in communities and by providers.

Standardizing Data

None of this can be accomplished without data. Therefore, AHCPR and others are involved in activities that deal with the improvement of data quality, standardization, and definitions. Yes, we have ICD-9 codes. Yes, we have DRGs. But, we do not talk efficiently, and we do not use those numbers uniformly across the country Insurance companies do not fill out standardized forms in the same way Often, insurance companies decide not to complete certain lines because the information is not necessary. For example, one of the country's largest insurance companies does not put any claims for ambulatory care in their huge HMO system because their program philosophy makes it unnecessary. That is, considering they are going to provide all the care needed on an outpatient basis, they do not need to keep details about the specific events.

So America, in its traditional way does everything quite, quite differently We sort of muddle through, but we can no longer afford to do that. We need to identify ways to balance the privacy of a personal medical record with society's need for better information on health care outcomes.

Balancing the protection of personal privacy and contributing to the greater good of society is not a new subject. It has been talked about by church and state for centuries. We in the health care field have talked about it extensively over the last 10 years, and now we need to go further. I would imagine that, collectively, you could make several recommendations about what might be done to resolve some of these issues.

Average Americans must be convinced that they will personally and collectively benefit by giving up a bit of privacy We must show that Americans receive the same kind of benefits from their health care system that they do when they give up a bit of land so the state can build a road. Help us, then, make a persuasive case to America that all of us benefit by allowing researchers to more completely know something about our medical records.

It is a challenge. I hope it is more than simply a debate, because we have had the debate before. What we need from you are specific recommendations that can be delivered with confidence to the American people. Indeed, this is a great charge, and I look forward to your results. ◆◆

Keynote Speech

Ruth **Faden,** Ph.D.
Professor of Public Health and Management
Johns Hopkins School of Public Health

In one respect, my task this morning is really quite difficult. I have been asked to set the conceptual and normative stage for our discussions. But in many respects, I am getting off easy. I get to lay out the grand issues, and then you get to work out the solutions and recommendations.

Specifically, I have been asked to lay out some of the foundational, conceptual, and ethical issues that are necessarily engaged in deliberations about privacy and information needs. The goal here, as I understand it, is to start us off with some common assumptions about core concepts and core moral commitments that can subsequently serve as touchstones for the less abstract, more particular discussions that follow.

My presentation is divided into three parts. I will begin with an analysis of the concept of privacy and the moral foundations for respecting privacy. That is, I will share with you some thoughts about what privacy is and the nature of its moral significance. I will then turn to the concept of confidentiality, where I will focus on the nature of medical confidentiality in particular, moral rules of medical confidentiality, and some of the large ambiguities that surround modern health record information that complicate efforts to explicate what rules of medical confidentiality mean today Finally, I will lay out some of the classic justifications for the infringement of obligations to respect privacy and confidentiality. I will also enumerate the kinds of outcomes that stem from attempts to resolve moral conflicts between such obligations, obligations to respect privacy and confidentiality and other deeply held moral commitments.

A Definition of Privacy

The literature literally abounds with many different competing theories and accounts of privacy. Others at this conference, including Alan **Westin,** Madison Powers, and David Flaherty, are much more expert than myself at wading through these murky intellectual waters. But for our purposes, one definitional account to which I am particularly attracted and that has served me well in my own recent work is the definition provided by Anita Allen. Allen defines privacy as follows:

> Privacy *is a condition of inaccessibility of the person, his or her mental states, or information about the person to the senses or surveillance devices* **of** *others. To say that a person possesses or enjoys privacy is to say that, in some respect and to some extent, the person or the person's mental state or information about the person is beyond the range* ***of others' five*** *senses and any devices that can enhance, reveal, trace, or record the human conduct, through belief or emotion:'*

The essence of this definition is to understand privacy as a condition or state of inaccessibility to others. A person experiences privacy when that person is inaccessible to other persons.

A person can be inaccessible to others in several respects. Allen distinguishes three paradigmatic respects, kinds, or forms of privacy: first, seclusion and solitude; second, limited attention; and third, information nondisclosure.

In seclusion and solitude, the person is physically inaccessible to others. By contrast, limited attention refers to the ways a person can remain inaccessible to others while still in their physical presence-for example, when we avert our eyes to avoid making eye contact with a stranger in a public place. Information nondisclosure, sometimes referred to as informational privacy, is the state of having information about oneself inaccessible to others. Confidentiality., a central topic for us in this conference, and secrecy are both species of information nondisclosure or informational privacy.

We should note that the way Allen and others explicate the concept of privacy is a morally neutral state or condition of the person, not a moral value. Indeed, some states or conditions

of privacy are undesirable or morally wrong, as when seclusion brings loneliness or isolation or secrecy reveals wrongdoing or harms others. At the same time, we often speak of privacy as unquestionably of positive moral value-as if losses of privacy **are** always bad and gains of privacy are always good.

Some losses of privacy can, however, clearly be good. For example, women are no longer confined to their homes for the last trimester or so of their pregnancy. They lost privacy; they gained freedom.

Invasion of Privacy-A Value-Laden Concept

The loss of privacy, per se, does not make it bad. But rather, something about the nature of privacy and the conditions under which it was lost makes it not merely a loss of privacy but an invasion of privacy. The term **"invasion** of privacy" is thus a shortcut for a highly value-laden concept defined as an intentional deprivation of a reasonably expected, desired type of privacy to which a person is morally entitled.'

When we use the language of rights to privacy and, correspondingly, obligations to respect privacy the concept usually concerns just such invasions. That is, rights and obligations to privacy are moral notions intended to capture those concept of privacy elements that we have in mind when we speak of invasions of privacy

Not only does literature on privacy abound with different accounts or theories of what privacy is, it also abounds with different accounts of the moral justifications or foundations for rules respecting privacy. The different kinds or forms of privacy-seclusion, limited attention, and informational privacy-highlight different kinds of justifications and moral values. Still, we can sketch the general moral considerations at stake in respecting privacy overall, and I will now turn to this subject. I have laid out for you some of the conceptual notions behind the language of privacy and now will speak a bit about what gives certain kinds of privacy moral value.

A Respect for Autonomy

One standard account holds that the primary justification for respecting privacy resides in the principle of respect for autonomy To respect the privacy of others is to respect their autonomous wishes not to be accessed or observed or have information about themselves made available to others.

Joel Feinberg has noted that, historically, the language of autonomy is a political metaphor for a state's sovereign domain or territory. Personal autonomy conveys the idea of a region of sovereignty for the self and a right to protect it. This idea is closely linked to ideas of privacy and the right to privacy and the notion of the sovereignty of the self. We talk about zones and spheres of privacy, metaphorical areas around the body and the person around which we claim privacy. Thus, the link between autonomy and privacy can be seen as fairly straightforward. Respecting privacy is one way or form of respecting autonomy. This straightforward link between privacy and autonomy does not, however, exhaust the relationship between these two concepts.

We can add a further dimension to this analysis. Respecting privacy is an important means of fostering and developing a sense of self, personhood, and personal autonomy Indeed, we have difficultly imagining how, in the absence of some amount and types of privacy, individuals can formulate autonomous preferences or, more basically, develop a **self-governing** capacity. If we are never private, we can never truly become ourselves.

On this account, certain privacy conditions are viewed as necessary to develop, or at least foster, personhood and personal autonomy. Thus, privacy is of instrumental value to the extent that it promotes personhood, autonomy, or self-governance. We need to be private so we can understand who we are.

Personhood and personal autonomy are not, however, the only or even the most morally significant ends promoted by privacy. Privacy enhances the development and maintenance of intimate human relationships-of trust, of friendship, and of love. Arguably, one of the defining characteristics of intimate relationships is that they involve the sharing, freely given, of private information, private spaces, and private acts. In an intimate relationship, we allow another to enter the otherwise private **sphere** of our lives. If privacy is not cherished and respected, both the capacity for and the meaning of intimacy in human relationships are clearly diminished.

As Charles Freed has argued, privacy is necessarily related to the ends and relations of the most fundamental sort-respect, love, friendship, and trust. Privacy is not merely a good technique for furthering these fundamental relations; rather, without privacy., these relations are

simply inconceivable. We cannot imagine what relationships would be like if there were no private sphere of life.

Today, we do not expect to resolve which is the more foundational moral justification for respecting privacy-the formation of intimate relationships, respect for autonomy or the development of personhood and the capacity for autonomous expression. My point is that privacy's moral value is mainly derivative and based on a complex of moral commitments and concerns. It is not simply animated by one moral concern or consideration, but by multiple moral concerns and considerations. This makes any analysis of when to override an interest in privacy all the more difficult. We are not talking about a single line of analysis that links a simple moral justification with a simple moral claim.

Protecting Informational Privacy

As I noted earlier, confidentiality is a paradigmatic means of protecting one form of privacy, informational privacy. The following account of confidentiality is obviously far less than a full definition. First, we realize that confidentiality is a condition or property of information-something about the information, not something about the person. The information is confidential; the person is not.

To say that information (I) about a person (X) is confidential is to say that the "I" is not disseminated beyond a community of knowers authorized by "X" to have access to that information. This analysis of confidentiality has an immediate moral content. The subject of the information authorizes some level of self-disclosure to specified, designated others but retains control over it. The information cannot be disclosed to others outside the community of authorized knowers without the person's consent-that is, without adding to the community of authorized knowers.

Rules of confidentiality require authorized knowers to respect the confidence with which they have been entrusted by not disclosing information to others without the consent of the subject of the information.

We have distinguished two ways that rules of confidentiality can be violated. The person or institution to whom information has been disclosed in confidence either fails to adequately protect the information or deliberately discloses that information to someone without the consent of the subject of the information.

Medical Confidentiality

Medical confidentiality is a special instance of general societal rules. Rules of medical confidentiality prohibit health care providers from disclosing to third parties information about a patient obtained in the course of treatment. These rules are among the oldest and most enduring medical ethics principles. They have a much longer history for example, than obligations to obtain consent for treatment or obligations to tell patients the truth.

For a complex of reasons, I am generally not fond of evoking the oath of Hippocrates. However, the oath's reference to confidentiality is one of my favorites, and.1 offer it with minor editing:

> Whatsoever *things Z see or hear concerning the life of persons in my attendance oj the sick, or even apart therefrom, which ought not* to *be spoken abroad, Z will keep silence thereon, counting such things as sacred. secrets.*

A commitment to keeping "sacred secrets" has continued in virtually all subsequent medical ethics codes, including the latest versions of the American Medical Association and the World Medical Association's Codes of Ethics.

At least five kinds of moral arguments have been used to justify these medical confidentiality rules:

- The rules of medical confidentiality should be **respected** as instances of general obligations to respect informational privacy.
- Medical confidentiality must be respected because of the special moral character of the doctor-patient relationship. That is, confidentiality is intrinsic to the very nature of this relationship, characterized as it is or should be by trust and intimacy.
- The rules of medical confidentiality should be respected because at least an implicit and sometimes explicit promise of confidentiality is imbedded in the institution of medical care, and breaking a promise is wrong.
- The rules of confidentiality should be respected because these rules are necessary to bring about good to patients and to society. Without this assurance of confidentiality., people would not divulge medically relevant information, medical care would be inadequate, and public health goals would not be served.

- The rules of medical confidentiality should be respected as necessary to prevent patients from the harm that likely could befall them if information collected in the course of treatment were to become publicly available.

We must recognize that only two of these five arguments appeal either directly or indirectly to privacy or privacy-related concerns, that the argument is grounded directly in privacy, and the argument appeals to the intimacy and trust character of the doctor/patient relationship. The other three arguments appeal to moral considerations quite different from privacy-related considerations-promise keeping, promoting the good, and preventing harm.

Thus, we have medical confidentiality rules not only because medical confidentiality is an important component of informational privacy but also because these rules advance other moral values-values other than interests in privacy. This is another reason why thinking about justifications for overriding ambiguities surrounding the contemporary meaning and application of medical confidentiality is very complex. The first contemporary ambiguity about rules of medical confidentiality in the modem medical setting is this: Who should count in the community of authorized knowers, and how does this compare against who does, in fact, have access to information? Although some commentators have increasingly argued that the rule of medical confidentiality is, at present, little more than a ritualistic formula or a convenient fiction, publicly acknowledged by professionals but widely ignored and violated in practice.

A Decrepit Concept

For instance, Mark Siegler has argued that confidentiality in medicine--I will use his phrase-is a decrepit concept. What physicians and patients have traditionally understood as medical confidentiality simply no longer exists. It is compromised systematically in the course of routine medical care. To make his point graphic, Siegler presented the case of a patient who became concerned about the number of people who appeared to have access to his record. This patient threatened to leave the hospital prematurely unless the hospital guaranteed confidentiality.

So Siegler set out to find out how many people, in fact, had access to the patient's record. He discovered that many more people than he had suspected had legitimate needs and responsibilities to examine the patient's chart. When he informed the patient of the number, approximately 75, Siegler assured the patient that these people were "all involved in providing or supporting" his health care services. All 75 of them had a legitimate need to have access to the information. The patient retorted, "I always believed that medical confidentiality was part of the doctor's code of ethics. Perhaps you should tell me just what you people mean by confidentiality"

We may be able to alter current care delivery practices to approximate more closely the traditional idea of confidentiality But a gulf is certain to remain and likely to become wider because of the need for information in health care delivery Patients doubtlessly understand some, though by no means all, of the institutional and societal constraints that limit confidentiality Under these conditions the patient should, at the very least, be informed about the meaning of medical confidentiality in the modem clinic and hospital setting, with its large and diversified health care team, its bureaucracy, and its multiplicity of third-, fourth-, fifth-, and sixth-party payors.

The second major ambiguity haunting contemporary interpretations of traditional obligations of medical confidentiality concerns when rules of medical confidentiality apply, in what context of health information, and with respect to what content. We are having enough difficulty figuring out what ought to happen to traditional moral rules of medical confidentiality as we move from the historical model of the physician, the patient, and the private office to the model of the clinic and patient and to the model of the hospital and patient.

Even more perplexing, what happens to traditional rules of medical confidentiality when we move from the health care institution to the drug store, to the workplace, or to the insurance company, all of which also maintain health records? Are such records confidential in some sense? Have explicit promises or assurances of confidentiality been made to patients and consumers? If not, should patients and consumers reasonably expect confidentiality practices? And if not, if patients receive no explicit promises or implicit social practices of confidentiality, what understandings of privacy apply?

Commercial Concepts of Privacy

This is a key issue for this conference. To what degree of privacy if any, are individuals entitled when health information is collected in a commercial, not

fiduciary context that does not resemble the health cam setting and the provider/patient relationship?

Whether, ultimately, we use the language of medical confidentiality and/or use the more general language of obligations to respect informational privacy in numerous instances such obligations will conflict, or at least appear to conflict, with other moral values and commitments. That is the subject of this conference.

For example, a personal health record may be accessed to prevent harm to an identifiable other party, to benefit the record's subject, or to benefit yet another person. More significantly, from a public policy perspective, this health information may need to be accessed to further a valued social good or community interest. And this I take, too, to be the core substance of this conference. This concerns such social goods and values as accountability and efficiency in the delivery and monitoring of private and public services, standard administrative uses, monitoring, and law enforcement. We are increasingly concerned about these kinds of issues in health reform. We need information to make our health systems more accountable.

We also occasionally value making personal health information public because of the public's general right to know. The interests of protecting a free press is a less often discussed issue, but one that is sometimes quite dicey. We also, arguably, need access to personal health information in order to advance science and medical knowledge, an interest that we, as community members, share. And, clearly, we need access to personal health information to advance the public's health, whether by controlling epidemics or by maximizing our investment in the health care dollar.

Value Conflict 'Outcomes

Now what happens when we have a conflict between any one of these interests or values and our obligation to respect privacy or confidentiality? There are at least four possible outcomes:

- First, access to information could be obtained with the subject's permission. You ask the person, "Can we have access to this information for this purpose?" In other words, you obtain a voluntary consent to loss of privacy. Because the person agrees to this loss of privacy we are not invading privacy.
- Second, the weightiness of the competing moral interests could justify access to the information. You would then have a justified infringement of obligations to respect privacy and confidentiality but no violations of these obligations. You would be justified in getting the information.
- Third, accessing the information may not be justifiable, but the information would be accessed anyway. In that instance, you would have a violation of obligations to respect privacy or confidentiality.
- Finally you may conclude that accessing the information is not justifiable and the information is not accessed. Here, no violation or loss of privacy occurs, but the related moral interests on the competing side remain unserved. Whatever you needed the information for would now have to remain unaccomplished.

A Note of Caution

I conclude my remarks with a cautionary note. Of the four outcomes previously mentioned, the most attractive is clearly to seek "consented to" access to the information. In theory, this alternative provides access to the desired information without violating any moral obligations and without the hard work of figuring out whether the privacy interests are indeed outweighed by competing moral concerns. You do not have to work very hard at the moral problem and the public policy problem. You seek permission, you get it, you get the information, and you go about your public policy business.

My cautionis that, as a practical matter, how much moral weight the typical consent to access information can bear is dubious. The catchall phrases in the waivers and disclosure statements read and signed by patients and consumers—"Your records will be kept confidential and will not be made available, except for statistical purposes," "except for research purposes," and "except for administrative purposes"-are doubtlessly not very meaningful to most people. Most people do not pay any attention to these clauses, do not attach any significance to them, and certainly do not understand a statistical or administrative purpose.

These statements must be made considerably more explicit, detailed, and practical with substantial public dialogue, so that the general public understands who has access to what

kinds of health information and for what purposes. If not, then these permission-seeking approaches will not do the moral work we would like. In other words, ***unless we*** do a good job of soliciting genuine informed consent or conducting an extraordinarily public education and exchange to provide citizens with an understanding of who now has information and for what purposes, getting consent will not get us off the moral hook.

In many circumstances, we cannot escape the hard work of figuring out how to balance respect for privacy with the need for information.

Endnotes

1. Allen, A. 1987. Uneasy Access: Privacy for Women in a Free Society. Rowman and Allenheld, Totowa, NJ.
2. Allen, 1987. ◆◆

Providers' Use of Primary Health Care Data

Roger Bulger, M.D.
President and CEO
Association of Academic Health Centers

The comments that we heard this morning make at least two points. One is that privacy is not a new problem. It is a problem that we have been dealing with in increasing fashion, and one that will obviously be exacerbated by technological advances and by the American people's many diverse needs and interests. The second point was the emphasis on the Hippocratic oath.

My job is to talk about the provider's use of data collected for routine provision of patient care. The provider's use of data is crucial to the relationship with the patient. The issue has its roots in the Hippocratic oath. Those quoted words are essential to establish a trust relationship, the common ground of any healing or therapeutic relationship that exists between providers and sufferers-those people we call patients.

Respecting Privacy

To actually care for patients, you must respect their privacy. This goes back to the very beginning of Western medicine. At the beginning of their careers, young physicians take the oath seriously; and from time to time, they take seriously the oath's renewal and the important things it emphasizes.

We are dealing with groups, however; I have seen abuses of what one might reasonably expect. I was reminded of that a year ago when I went to the Mayo Clinic for the first time. I was just visiting and wanted to see how the records were handled. It was a very impressive place with a very impressive philosophy and a very impressive array of patient commitments. I was escorted by someone who was not a physician and not accustomed to escorting visitors. In the records room, I wanted to see how a record was kept. Every one of my instincts allowed me to do that because, in places where I had been medical director, I looked at records all the time. But I was not allowed to look at the record; no one was. The organization had a very strong commitment to privacy. I was told that if people are overheard discussing a patient in a semi-public place, they could be fired.

I came away thinking that if I were a patient in a place that took such care with the level of privacy, then my comfort level and maybe my potential for healing would be very much enhanced. Knowing that all the care givers were operating and sharing in that position would be very comforting. This, I believe, is the first lesson.

The other side illustrates another situation. About 30 years ago, I was at a brand new university hospital and was trying to do everything right. We had the latest dictating technology The doctor and the nurse could actually dictate; they did not have to write notes.

This hospital took the precaution of sending the dictation drums 500 miles away for transcription at considerable expense so that the typists would not be in the hospital. These recordings included very personal records from various psychiatric notes. One of the typists, 500 miles away, was reading of the phenomenal sexual exploits of a woman patient who, it turned out, was the wife of the owner of the typing business. There is no way to have recovered anything from that-it was an absolute shambles. And, yet, everything was done with the very best intentions.

The Inevitable Human Error

There is a message in this. No matter how hard we try, some errors will be made. The things with which we are currently dealing may compound those kinds of errors. Willis Ware, I am sure, will tell us many things we can do to protect and secure records. But even then, nothing will prevent the error that no one anticipated—the human error. Nothing will prevent people

from being sloppy and less than optimal in their behaviors unless we turn to that task with greater vigor. This is one of the most important things we need to do as we become even more technocratic.

We have clearly broken confidentiality in the usual one-to-one relationship through research and through the groups of people who must have access to the files. We have talked about that, and I will not dwell on it. But we must be able to trust others with information, especially when someone is very sick and circumstances are complex.

Now we are moving to a larger dimension where data can be nicely distributed. We all are learning gradually, sometimes to our horror, how widely dispersed our financial records are and how easily accessible they can be to those who really know how to work with computers and break codes. Such issues affect our current problems and contribute to creating the relationship between the individual and the individual's rights and society and the societal good.

The societal pressures are increasing, and many of us feel almost lost in the spiraling cycle of technology. In a recent essay, historian Daniel Boorstin describes America's contribution to the world culture as being centered on technology. He calls it a republic of technology, wherein communication between peoples is through and with technology This implies a sense of progress and improvement and draws citizens away from any doctrine or credo to govern and control life. The pursuit of technology in America, almost a population-wide commitment to be the world's innovators and self-experimenters, takes the place of commitment to doctrine. That is what he believes.

Technology-Our Genetic Makeup

This interesting and impressive essay starts one thinking about how technology is intertwined with our society and how it has almost become a part of our genetic makeup as a nation. Boorstin describes the incredible Philadelphia Fair of 1876, opened by President Ulysses S. Grant—Grant pulled a switch and started approximately 18,000 different engines all at once-and how this whole approach is a way to deal with the future, with hope, and with progress. Although we are beginning to understand the limits of technology, we are deeply involved in it.

One hundred years later, Howard Nemerov, Poet Laureate of the United States, wrote these lines depicting the tendency to glorify the inventor and developer, rather than the evaluator and the critic:

> *Praise without end for the go-ahead zeal*
> *of whoever if was invenfed the wheel;*
> *But never a word for the poor soul's sake*
> *that thought ahead and invented the*
> *brake.*

Here is an opportunity to think about relevant brakes and how we can deal with our current environment.

We must accept the fact that our technology and capacity are tremendously valuable. Of great value is information, computer linkages, electronic capacity, and the ability to take personal information and relate it to the population. Such information will not only go to the insurer, the payor, the researcher, and the evaluator of trends, benchmarks, and quality of care, but it will feed right back in real time to the provider. And so, you ask, "Well, what's useful for the provider?" I believe we must value the whole chain of information. Let me explain.

The Chain of Information

A recent paper described how doctors and nurses alternated in entering the medical record of randomly selected patients into a hospital's electronic system. A comparison of the electronic and manual system showed an approximately $900 per-patient-visit savings with the electronic system. Although people could read the doctors' orders, reading took longer with the manual system. When you put information into the computer, others can read it accurately The drug data in the computer can be tracked by many persons for multiple purposes; the computer provides valuable feedback from many sources. Cross reactions can be prevented. A doctor can find out what other prescriptions a patient may be taking. The electronic system offers a whole host of real-time advantages.

Advanced information systems offer another opportunity for development—postmarketing surveillance of drugs. A drug approved to lower, your blood pressure promotes hair growth, for example. Everybody uses it to grow hair; nobody uses it for blood pressure. Then we find out that when you give it to 20 million people, 160 will develop a secondary problem and their umbilicus will disappear. You would not have noticed such a small number of adverse effects in the normal drug followup. The process

that tracks these approved drugs in such detail is called postmarketing surveillance. We do not do it in this country; we have no good way of doing it. This is an obvious advantage of great importance and great significance to electronic data systems.

In another example, someone comes into a physician's office with a sore throat. The physician does some cultures. By feeding this information into a shared database, almost instantaneously the physician can retrieve data indicating that during the past month 70 percent of city residents with certain symptoms did or did not have beta hemolytic streptococci. So when a physician can link the patient's data into the larger population-based data, patients receive a whole host of real-time, valuable, practical benefits.

Letting Patients Control their Destiny

We have many, many things to talk about, including patient autonomy. The future in which we are now imbedded, and cannot escape, is to increase patient control of his or her destiny. I think much of the information that the patient needs can come out of these electronic databases.

Many have heard of John Wennberg's studies in which he offered an interactive video disk system to people about to have their prostate removed. The system helped explain the procedure and discussed outcomes. Wennberg studied patients who had the system and the operation and those who did not have it; patients who chose the procedure and who did not; patients who talked about the complications; and patients who talked about what it did for them and what it did not do. The disk takes about an hour and a half. No doctor is able to inform patients as well as that video disk. As a result, many people got off the surgery line and stayed off, deciding that acceptable practice indicated it was legitimate not to have surgery.

Information and data that increasingly emerges from our large data sets about appropriateness, available options, and complications will empower patients much, much more so than now. Paradoxically, this improves patient autonomy and improves shared decisionmaking among doctors, patients, and payors. As providers face this future, they are increasingly afraid of the lawsuits because of so many complications. We know that this alters people's behavior. In general, as people become better informed, providers will respond. But care must be taken as we do this.

I will just leave you with one lesson from the great Yogi Berra-many of you baseball fans will remember his famous non sequiturs. For years, I thought Berra, the great baseball player, was actually dumb. But he is very quotable, and it turns out that he may have been a lot smarter than we thought. One of his gems emerged during an interview when he was asked, "Now, Yogi, you have a son. What did you tell him about life?" And he said, "Well, I'll tell you. I actually did tell him something that was important. When he was 16, I said, 'Son, when you come to a fork in the road, take it."'

Now I know you are quicker than I am, but I want to interpret that one more step. In fact, in some cultures, people would come to a fork in the road and not take it; they would elect to stay there, frozen with indecision over which path to go down. We are still Americans, enhanced by our belief in progress and improvement. We are going to go down a road; we are going to take a fork. The question is how to design the steering and braking mechanisms correctly so that we can stay on whatever fork we do take. ◆◆

Providers' Use of Primary Health Care Data

Peter C. Waegemann
Executive Director
Medical Records institute

A couple of years ago, a journalist was researching a personal story about a famous movie star. The journalist had a hunch that something had been done to the star in a New York hospital. He took a white coat, pretended he was a physician, went to the hospital, obtained the actress' medical record, and published that she had VD. She had the means to hire lawyers, and she sued the hospital. She got a $640,000 settlement because she proved that she lost a commercial project to advertise some makeup. She got a year's payment. In the meantime, several years had gone by, and she lost out. This case had been personally traumatic to her.

In another case, in 1992 a very famous woman in the Boston area, well-known to most people through television and politics, decided to have a breast enlargement. She planned it very carefully since she did not want anyone to know. She told friends, a television interviewer, and her church that she would be going to Hawaii for a week's vacation. She took all kinds of precautions to make sure that no one would find out.

She was admitted to the hospital, which is part of a church-run, church-owned operation. The local pastor was immediately notified-the standard practice when patients were admitted. This pastor knew his parishioner quite well and knew that she was supposed to be in Hawaii. So the pastor went to the hospital to see what had happened to this patient because he was concerned that she had had an accident or some other traumatic incident.

What we have here is an embarrassment. The woman could not sue anyone; she did not want to sue anyone. Her personal career was certainly somewhat set back as a result, and she was lucky that the Boston press agreed not to write about it.

In a case that occurred very recently an ambitious political candidate was anxious to gain a post of high political exposure here in Washington. Researchers looking at his personal data accidently found out that some 26 years ago he was admitted to a mental institution. No one knew for how long; no one knew for what reasons. His case was dropped. He was not considered even for the inner circle of candidates. He could not sue; he could not do anything about it.

Finally a case from Colorado is the worst case I have ever known. A medical student lived or shared a room with an attorney who made his living handling malpractice cases. The attorney considered it important to review medical records before clients came to his office. If he could see in advance that the case had some merit, he could say "All right, I'll take this case on for $2,000 down and 20 percent of the outcome." If he could see in advance no real good hope, he would say, "I need $5,000 down. Otherwise, I don't want to spend any time on this, and I need a substantially higher amount of the outcome."

His friend, the medical student, now says she does not really know how many records she copied at night-it may have been about 2,000. She had sold them for up to $50 each to additional attorneys in Colorado as well as to out-of-state attorneys.

The point I want you to remember is that she was asked to leave medical school. And what did she do? She entered law school and is now a district attorney in Colorado.

Consumer Protection Violations

We have legislation that clearly describes consumer protection in regard to credit information and other different areas. When someone violates a consumer's right to privacy, this is automatically a crime with certain minimum penalties. When we talk about health care, none of that exists. If you are lucky enough to have a

case where you can sue, you might get something out of it. If you do not have the means to sue or if you do not have a case, too bad.

All of these cases involved paper-based records. The move is on toward computer-based patient record systems. The benefits are clear. We are looking for better health care and improvement in quality of care. We are looking at cost savings. We are looking at a number of advantages. However, we need to realize that the dangers of a computerized patient system cannot compare to any paper system. Databases can be broken into; they can be accessed. Most people are talking about a longitudinal patient record, a record from prenatal to postmortem. Can you imagine, if all the data from your psychotherapist to your OB/GYN clinic were in one place, what a tremendous issue it would be to safeguard such information? And electronic patient records provide easier access to people who, instead of copying one record at a time, can potentially take hundreds or thousands of records and sell or misuse them.

Essential Legislation

In looking at computerization, we need three pieces of legislation. The first-one that everyone is currently talking about-is a new piece in health care reform that comes up with solutions towards access to health care, cost, and related issues. Many people are working on that.

The second piece is equally important-I call it legislation to enable computer technology We need federal legislation that overrides state laws that still dictate pen and paper in many cases and that make it possible to have a clear understanding of data integrity on computer systems. We need legislation that will deal with computer signature, computer use, who can access it, who can use it, and legislation for computer retention and permanence of information.

We can learn from some of the European countries, particularly France, that have what they call the "card professional," issued as a smart card. The card is issued by a fee licensure organization to each physician or health care professional. The professional uses it as a key to access information he or she is entitled to because the information is necessary for care. The card can be used as a computer signature. The French use of the smart card may not be the only way to solve the problem, but we need legislation and we need it quickly to enable the computer system and the health care professional to interact effectively.

The third piece is confidentiality. At this point, we really need to look at a number of issues. What potential harm is being done to the patient? We need to have a clear understanding of the dangers in the United States, not to mention those in Europe. I could describe the horror stories coming out of East Berlin, where the Communist Party and governments in Eastern Europe have constantly used medical records to destroy people-not just professionally They destroyed them as persons-they altered information and used it to destroy individuals who did not agree with the regime or political views.

This is so far removed that we cannot imagine it ever happening in this country. However, some people are concerned about underground organizations gaining access to information and using it in the same ways communist countries historically used it.

When we disregard the first issue, professional ruin is left. Here again, cases occur where physicians are mistakenly identified as being HIV positive. The next day, patients cancel appointments, forcing the physician to give up practicing medicine, at least in that state and under the physician's original name.

An individual's career or credit worthiness can also be ruined or damaged. In a number of cases, banks or credit organizations have not given individuals credit because they felt that the individual would be unable to pay back a loan or to keep up mortgage payments because of a known illness.

Accessibility of Longitudinal Records

Can you imagine a longitudinal health record situation where everyone has their complete medical record accessible? If an employer wants to see an individual's health record going back to high school or earlier, and if there is one dark point, that person may not be given the job. We need to make sure this cannot happen.

The most common cases involve the negative image in the community, the personal embarrassment. I have seen two or three estimates saying that a case of personal embarrassment happens not just once but maybe even twice a week in this country-someone is being personally embarrassed because medical information has been leaked or exposed.

So what do we need to work on? We need to first have an understanding and a consensus on the potential harm. Secondly, what information can be harmful? And here again, we need to look

in more depth. Some people say, "Well, it is only the sensitive information. It is only substance abuse or OB/GYN information." An individual's acknowledgement that he was admitted into a mental institution or into a rehabilitation clinic can, by itself, be very damaging.

We will be looking into the methods of information access and dissemination that can lead to violations of privacy. The next point is to come up with some general confidentiality measures and invent some kind of practical guidelines that can be used by the future computer implementer and by the developer of computer systems.

Uncontrolled Access

A number of issues concern uncontrolled access by health care professionals. As a nation, we need to look at where to draw the line. In Europe, confidentiality is being put into legislation in a way that would never be acceptable in this country. In France, a physician may only give another physician information that a patient has previously approved. If you are HIV positive and you say to a physician, "I do not want you to tell this to anyone else," so be it. That would probably be unacceptable in this country.

You may have heard about the case in Texas where a patient had cardiac surgery A specialist was flown in and immediately helped in the surgery. When the surgery was over, the family was told, "We have good news. Your father is in reasonably good condition. We had to call in Dr. X, a specialist from Houston." The family sued the hospital for $3 million. People asked the family, "But do you not agree that this specialist helped your father?" The response was always, "We do not know what he did to us." It turned out that the physician's family and the patient's family were neighbors and had been fighting over a piece of land for 85 years. After three shooting incidents, nothing had been resolved.

We must understand that the physician, in many cases, is now being considered "just" a human being-not someone who automatically has access to any information-and a patient has a right to deny certain health care professionals involvement in their care and access to information. This needs specific regulations.

We must resolve the question of how information is being disseminated between individuals, organizations, administrative personnel and employers, and additional parties, such as insurance companies. This involves general measures for controlling confidentiality.

You have already heard that we must find a fine balance between the need to know and the right for privacy implementing confidentiality. But there is a third issue-the economic issue. In the past many people have seen or believed that computerization automatically means a lack of confidentiality. It does not have to. Instead, computerization is only a question of money. As a nation, in the next couple of years we must wrestle with this question: If we should create an electronic patient record system costing a hundred billion dollars, are we willing as a nation and as individual patients and providers to spend 10 percent, 15 percent, or only 5 percent for confidentiality measures? In dollars, those numbers are $5 billion, $10 billion or $15 billion. These are issues that must be put in relationship to what is being done. ◆◆

Providers' Use of Primary Health Care Data-Discussion

Roger Bulger, M.D.
President and CEO
Association of Academic Health Centers

Peter C. Waegemann
Executive Director
Medical Records Institute

■ **Participant:** I have a question for both of the speakers. First, I was delighted that Dr. Bulger explained the meaning of postmarketing surveillance. The term is enough to send shivers down the back of a privacy advocate. Although it involves marketing and surveillance, once it is explained, one cannot oppose it. I am considering ways in which postmarketing surveillance can be intelligently conducted within data protection rules.

The other examples cited, such as monitoring prescription uses, illustrate the need for such surveillance as well as the need to set up proper data protection measures to conduct such monitoring.

With respect to Mr. Waegemann, I wonder if he is aware of French data protection rules and whether France has developed detailed rules for medical confidentiality that are helpful within the general framework of the **1978** law?

■ **Dr. Bulger:** I was trying to present some examples of current and future utilities. But, I understand that patients might not be entirely happy about having all their prescription records accessible. This raises some questions that need consideration.

I am not sure I have thought that all through. I am also not sure that surveillance is as pure and good as I described it. It is entirely possible that people would like to maintain their prescriptions under their own control, go to different doctors for specific reasons, and be in a situation where they could prevent the pooling of personal information.

So although I am glad that you agree it is good-1 also think, in general, it is good-1 am not so sure that it is an unalloyed good in every consumer's view.

■ Mr. **Waegemann: I** mentioned France particularly in regard to what I call the computer enabling act or computer information act in health care, which is needed in this country. I think we can probably look at that. The way they have approached the smart card problem might help us become clearer on similar issues.

When we look at confidentiality, it is worthwhile to look particularly at Sweden, Germany, and the United Kingdom. All these countries have created positions of data protection ombudsman or data protection commissioners to satisfy the needs of their respective societies. Data protection commissioners in countries like Germany and France hold cabinet level positions. Their sole responsibility is to protect the patient and consumer and make sure that all information-related work is filtered, if you like, through this administration. The same countries are implementing these programs at what could be considered the state level. So if we really want to take that example, we would need similar implementation of data protection commissioners.

■ Participant: Collecting data and creating a longitudinal picture of someone's life could be considered an invasion of privacy. I am thinking particularly of incidents of **mental** illness or other sensitive events, like an abortion. To have all your records available to a physician seems like overkill; some standard should indicate what is relevant to the current case and what is accessible.

I also have serious concerns about data sharing. Consider the example of pharmacy records. If I am the patient and you, **as** a doctor, say to me, "I need this information. We will keep it confidential, we will only combine it with other

records that are relevant and only give it to people that are qualified." Your office has a connection with a pharmacy. The pharmacist has a computer and finds it advantageous to connect with other pharmacists across the country and see which drug they sell the most. If that is done, which likely is a good marketing strategy, where is the protection of the person in that whole scenario? Once these databases are built, when is access limited? And, also, how do you specify that it can only be used for this purpose and no other purpose?

Regarding consent forms, I have looked at several and done a little research on the topic. The average citizen in a physicians office often signs consent forms releasing information under pressure, under the perception that not signing the forms will decrease the quality of care. An element of coercion may be in that kind of interaction.

Finally, if you really want to improve the quality of health care, the patient should have the right to access longitudinal data about his or her health care provider's performance and quality of care.

■ **Dr. Bulger:** Very good comments. One of the advantages of this kind of information, and what I was hoping to convey, is that as we collect data on outcomes of practice and feed it into larger databases, we can remove the individual's name; but all the data can, in fact, be returned. And that is what I was referring to when I said patients should be empowered to gain more control over the **payors** or providers of the system, over what they are buying and what options they choose in their care, and over whom they choose-assuming the system allows them that-because that information can come back.

The data we collect now is in a very rough form; we can read the hospital mortality rates associated with diseases. We know that data is very crude and can be massaged and made more sophisticated. We are in the process of doing this throughout the country. Many current activities are aimed at providing just what you **want—** more information about the provider and more information about how effective that provider has been with your problems.

The information that will create the longitudinal story will remain forever accessible. This is an extreme difficulty, and I will be interested in seeing how my colleague deals with it.

■ **Mr. Waegemann: What we** really are wrestling with here is a question of what actually is the longitudinal patient record. At this point, we do not have a clear consensus on what this animal is going to be like. In the United States or even in Europe, we do not have any concept model of the electronic patient record, what it consists of, where its subsets are, and other factors.

There are several issues. First of all, with a longitudinal patient record and different disciplines putting information into it, the record can be safeguarded by the "draw effect." In other words, only a patient providing a personal identification number (PIN) can allow certain parts of a record, like mental health therapy information, to be accessed by the health care professional.

Of course, an overriding mechanism can be built in to guard against situations where a patient is not able to provide the PIN. This makes it more complicated. But by having this kind of mechanism, you can make sure that your dentist is not looking at your OB/GYN record.

The second issue we must wrestle with, particularly when focusing on confidentiality, is where to locate the home base of that longitudinal patient record. Should it be stored within your current provider, your HMO, your hospital, your family practitioner? And where would it be updated? In the provider setting? Would it be located, as with some states and areas, within a communitywide health. information system with a state or regional database and information system?

The next question is-what kind of ownership exists? What rights does the patient have to the information? I could tell you stories about patients incorrectly accessing their medical record information,

We need to wrestle with the issues of ownership, location, patient access, and how to have certain subsections that are only available by having an "additional key."

■ **Participant:** A backdrop to this conference is the rising consciousness about privacy among an increasing number of Americans. A primary reason for this is, as Mr. Waegemann pointed out, that **when people discover they do not have rights, they start getting very concerned about it.** When they have rights, they do not worry about them any more. When they do not have them, they want to recover those rights.

In that light, it is important to challenge some conventional wisdoms. We always talk of the costs of privacy. It was good to assign percentages to the costs associated with privacy Conventional wisdom handles these privacy issues as they arise, as an afterthought, or as a little side issue.

But with the rising consciousness, I would like to point to something that happened a few years ago. Equifax and Lotus Marketplace were investing millions of dollars to put almost the entire consumer country on a CD ROM, so anybody would be able to have your name, address, estimated income, and shopping habits on their shelf. When word about this got out, 30,000 people protested. The companies had to withdraw the whole project because it really touched a nerve.

With the two conventional wisdoms of the cost of privacy and handling privacy as an afterthought, we still have to ask: What are the costs of not dealing directly with the privacy issue? Considering the example of Lotus Marketplace, could there be such a backlash about a privacy scheme that this basically good project of trying to computerize these records is derailed?

Do you foresee the failure to address privacy as something that has a potential to derail this in light of the Lotus Marketplace model?

■ **Mr. Waegemann:** I know of five major computer projects that are not being pursued because people did not know how to deal with confidentiality. Two Canadian projects would have involved computerizing the whole province. Germany planned to have general patient cards, insurance identification cards, issued to' its citizens. Parliament ratified the law and by January 1, 1992, every person in Germany was to have an identification card. Because of confidentiality problems, no identification cards have been issued, the whole project is stuck, and no one knows how to get out of it.

■ **Participant:** I work at the Albert E. Trishman Center, a national resource center for people who work with troubled children and their families. The mission of the Trishman Center brings up an issue that I have not heard yet-that of children and real concerns.

Mr. Waegemann, you broadly mentioned potential harm regarding confidentiality, particularly involving an individual's career. I suggest that we start with an individual's life, access to education, housing, and basic safety in the world. We have real serious concerns about what happens when information about histories of sexual abuse or sexual perpetration or something along those lines-starting perhaps at age four-is made readily available to people and how that would affect an individual's ability, for example, to get into high school and college.

I am also very concerned about and hope that one of the panelists will address the fact that this is a DHHS hearing. Children and families are seen in departments of human services for mental health servicing. I have a real concern about places like residential treatment programs, family service centers, and community mental health centers servicing children for this kind of treatment, using Medicaid, and the implications regarding computerized records.

■ **Partlclpant:** In most hospital settings where patient records have been electronically converted, there is a need for a measure of quality, some measure of outcome, and some demonstration of a reduction in cost as a result of improving communication among professionals in the care of one patient.

In the case of the primary care record-that is, a record in an ambulatory setting where problems are far less identifiable-they tend to be quite broad without clear interventions that always work or set standards for how things can work. In this setting, how do we measure whether or not making that record electronic has value? How do we demonstrate an improvement in outcome quality a reduction in cost, and the risk to confidentiality in making those kinds of investments?.

■ **Dr. Bulger:** That is a very good question. The answer is that all of those things have yet to be demonstrated. Studies will need to be done as we go through the processes. With the way health care is going, specifically the hospital part of care, one can draw out a scenario that has the hospital shrinking to a large intensive care unit for specialized cases, and the rest of care being carried out in the ambulatory setting. Clearly, access to the critical data of someone's EKG, hematocrit, and infection history is frequently useful and important to the patient. It is valuable information and can prevent duplication and waste.

I am not saying, however, that going from a written record to an electronic record in the standard encounter has at all been shown to be super useful. I think you raise a very good question.

■ **Mr. Waegemann:** There are two issues that we really should not spend too much time on because neither is directly related to confidentiality. A study published by Dr. Clement McDonald shows computerization can save up to 15 percent in health care on tests and such. Secondly, the Computer Based Patient Record Institute is working on these issues, and some members are here today. We should acknowledge the work being done there.

■ **Participant:** I want to make reference to one of Mr. Waegemann's stories-the experience of someone being considered for high appointment and rejected after the appointing authority somehow found out about psychiatric treatment. The chances are that the individual was asked directly about that. The form attendant to getting even a very minor clearance for a nonsensitive government job includes the applicant's consent to giving the government access to the entire medical record. We may not need to debate that here, but this issue will have to be addressed when we do the balancing.

■ **Mr. Waegemann:** I believe the information was actually obtained through an interview with this man's ex-wife.

■ **Participant:** All right, and the chances are that the investigator's standard interview format included a question like that.

■ **Participant:** I am a computer scientist. We currently use the partitioning of data between primary health care providers to improve the quality of health care and to hold down costs. We use the second opinion to get an improvement, either in cost or in quality of care. How would you propose to do that in a complete patient record that does not have barriers erected for these purposes?

The second question is about the hundred billion dollar figure thrown out. This makes nuclear weapons sound like a bargain. I wonder if you can cite where this cost figure came from?

■ **Mr. Waegemann: You** all can access the HCFA study published in October that estimates about $50 billion. If you expand all the areas that have not been accepted or reworked, assuming that it costs about $10,000 per hospital, and look at various formulas, you come up somewhere around $70 to $100 billion. I believe more around $100 billion because the European community assumes that just creating the necessary communication network will cost around $80 **billion. The cost is somewhere** between $50 and $120 billion, but at this point no one knows.

We, and particularly this Administration, need to make clear to the general population the tremendous benefits the computer-based patient record promises and that the effort is so great it only can be compared to the space program of the '60s. We really need to look at the efforts and resources needed nationwide to achieve that.

■ **Dr. Bulger: In answering an** earlier question about primary care, one needs to remember that many of our health care costs are created by the little things done frequently that go unnoticed. For example, in this country some 50 or 60 percent of women- get Pap smears perhaps twice as often as they need to and 25 percent never get them. At least if we were able to computerize and easily audit primary care sites and training, we could begin to look at things like this and make **sure** that a certain level of quality was better assured.

■ **Participant:** As a primary care provider, I am looking at things from the other side. Perhaps you should issue all health care workers a big silver badge and a gun and allow them to shoot anyone who uses health care data inappropriately-the journalists, the lawyers. Is it our responsibility to pay billions and billions of dollars to lock up data so that other people cannot use it for their own personal gain?

Regarding sharing of data among professionals-many times a colleague will say "I had an interesting patient last week. A young man came in with a multiplicity of symptoms, so I did the whole workup-neurological, laboratory-and ran up a $5,000 bill. I called the patient back and said, 'I am sorry I have to tell you this, but you have a serious disease. You have. ..' And the patient said, 'Gee, that is what the other doctor told me last week."' How many times will this patient rob the system of **$5,000?** How many **well-**baby checks is that? This is an issue that society must deal with.

Professionals are empowered by society because they have a certain body of information. Their goal and responsibility to society is to use this information to better society. We are looking at technology at databases, at large advancements, at electronic data transfer. We are looking at the possibility of manipulating large databases.

However, society's fabric is changing. It changed with the industrial revolution and it is changing with the technological revolution. Our job today is to help reweave the fabric of society. I do not think that we are that far off base. Consumers want responsible health care; health care providers want a responsible consumer. Our goal is to educate the consumers and the providers to the fact that this can all work together for everybody's gain, and we can do it very economically

■ **Mr. Waegemann:** Just a quick response to Point 1: yes, I agree, we have to decide that no one really knows. Point 2: I think the health care reform might take care of it, and we hope that this is being addressed.

That gives me a chance to make one comment myself. We should be aware that we are talking about confidentiality-it is a question of the social security numbers. Currently all legislation on the Hill is proposing using this number in the future; the patient is being identified with the social security number. A number of people, including myself, see potential problems of confidentiality, because you can link an individual much easier to any specific data, similar to a provider numbering system. ◆◆

Health Data and the Private Sector

Lorna Christie
Senior Vice President
Direct Marketing Association

Many of you are probably wondering what someone who represents direct marketers and mail order catalogers is doing at a conference on privacy and health data records.

Well, there is a really good reason why I am here today. Steve Brooks is a direct marketer. Aetna represents many direct marketers who happen to use direct response techniques to market their product. In Steve's case, the product is insurance.

In addition to talking about privacy, I would also like to introduce another subject-fair information practices and the principles behind fair information practices. Those practices and principles are particularly important when dealing with something as sensitive as health data, and particularly when talking about the collection, use, and dissemination of that data.

Before addressing the specifics, I would like to broaden the scope. Direct marketers really represent every segment of the American economy. Very few Fortune 500 companies today lack some type of direct response branch. We rely on information to reach our consumers and our customers; we are not the corner drug store. In many cases, the company that the consumer has a relationship with is halfway across the country. In other cases, the company may be halfway around the world.

I have a unique job for a trade association, and I am told it is a perfect one for someone with my personality. I get to tell the industry what they are doing wrong. I also get to tell them, however, what they are doing right and how we can spread the message of positive information practices and principles throughout the industry.

We are here today to talk specifically about privacy. What is privacy? Everyone in this room would probably give me a different definition. Because we rely on information, we have focused on the issue of privacy for a long time. Many of you may believe that it was just invented in the '90s. Privacy became an issue for us the day we started collecting the first customer information.

Defining Health Data

In combining the problem with defining the term privacy for the individual consumer, I will throw in another problem. How do you describe or define health data? Most of you feel, and I certainly agree, that health data is, by nature, more sensitive than other types of marketing data available in the private sector. But, yet, we have the problem of consumers filling out surveys and voluntarily giving marketers specific prescription information. So is that health data? If it is, it certainly was not sensitive to that individual consumer.

What we have to do is gather a lot of data and find the balance between consumer privacy expectations and the use of information for marketing purposes. In 1973, HEW established fair information practices principles. I go over them today because they are very important. These principles basically were to minimize intrusiveness, maximize fairness, and create legitimate expectations of confidentiality. While the original principles were written with regulation in mind, and how to make this regulation effective, the Direct Marketing Association (DMA) achieves these goals through industry self-regulation.

For direct marketing, privacy is indeed a customer service issue. A trade association professional must educate our members on the value of self-regulation because it allows them to respond to their customer needs; Therefore, it is a bottom line issue and not something this industry takes lightly

We accomplish self-regulation through many means. We have personal information protection guidelines. These guidelines are also incorporated into the ethical guidelines of other marketing segments, such as mailing list practices and telephone marketing.

We also have a new product in the evolutionary phase of self-regulation-a fair information practices checklist. This checklist is designed specifically for companies with an internal audit. It consists of steps a company can take to make sure it is meeting consumer privacy expectations.

Value of In-house Suppress

We also have established programs on the value of in-house suppress. In-house suppress gives consumers a sense of control at the point their name enters the information stream. In other words, as soon as I subscribe to something, as soon as I buy something, if that information is to be used for other marketing purposes, the Direct Marketing Association believes that I have the right to know that the information is being collected and how it may be disseminated. This is particularly important in dealing with data that is sensitive, such as health data.

These programs have become the standard for other trade groups and associations around the world. Indeed, we have an annual summit of trade associations to talk about what we are doing right, self-regulation, and how we can improve the programs.

They are not perfect by any stretch of the imagination. If they were I would not have a job, because part of my job is to manage those programs. More importantly, my job is to improve those programs. How do I know the programs need to be improved? The marketplace tells us the areas in which we need to be stronger.

We also have a DMA privacy action plan that specifically addresses the privacy issue and how our self-regulatory programs can be improved to respond to consumer privacy expectations. We are aware, and the members of the direct marketing industry are firm believers, that the types of information that should be collected and used for marketing purposes have limits. Our guidelines for ethical business practices state that directmarketers should be sensitive to the issue of consumer privacy and should limit the collection, rental, sale, exchange, and use of information to only those data that are appropriate for direct marketing purposes.

We also go a step further. Information and selection criteria considered personal and intimate by all reasonable standards should not be made the basis for rental, sale, or exchange when the consumer has a reasonable expectation that the information will be kept confidential.

We actually administer the guidelines. In researching the file, we have found set cases in which health data was used to violate consumer privacy. In one particular example, a blood bank in New Jersey decided it would be a good idea if they marketed lists of consumers who had had blood tests. This company had no idea of the consumer privacy sensitivities; this issue was looked at solely as a marketing practice. The DMA guidelines or the DMA committee was able to educate that company, to raise its awareness that it had a responsibility when collecting that type of information not to disclose it for outside marketing purposes.

This illustrates a very important point in managing consumer expectations and the issue of health data in the private sector. We do have cases of nontraditional direct marketers who are using and marketing information inappropriately Those situations are not widespread, and in most cases, self-regulation is able to deal with them.

In general, all data can be developed in two ways. Information is compiled on consumer buying patterns such as business-to-business exchanges or usage patterns such as in the medical professions. Data can also be developed through surveys, club memberships, pharmacies, and sign-up sheets in doctors' offices. These examples clearly illustrate a very important point in data collection.

The Right to Collect Data

Yes, marketers do have the right to collect data. America is a fairly open information society; many have argued that is why our country has been able to compete. But with that right comes a responsibility; that responsibility is to inform consumers through disclosure practices. Marketers also have the responsibility to be aware of the limits of the exchange of sensitive information, like health data, particularly when it has a negative impact on the consumer. Even with the perception of a negative impact, marketers must design their programs with that in mind. When you are dealing with something like privacy the consumer does not differentiate between perception and reality. If the consumer thinks the marketer is doing it, it is just as bad.

Member segments, such as insurance, have a need to access health data information to serve their clients; but most traditional direct marketers have no need for health data. Even in the case of the insurance companies, the information

used to target potential customers is generally derived from demographic data, not specific health data. Business-to-business marketers may rely on prescription drug information; for example, what types of physicians use what type of drugs to market to physicians. In that case, the patients' names are deleted long before the data is used. Indeed, researchers have been very hard pressed to find specific cases of violations by pharmaceutical companies in their marketing practices.

I am not saying that abuses do not exist. Misguided marketing practices do happen. But in this case, we have found that they are in fact misguided marketing practices by over eager sales reps or over eager marketing professionals who do not understand the need for balance. And getting back to the responsibility issue, companies have a responsibility to train their associates in fair information practice standards.

We have also heard stories of 800 numbers being used to collect data-not on prescription drug information, but on whether or not you suffer from hay fever. The consumer has a right to know if this information will be used. And also, you have the situation of consumer sign-up sheets in doctors' offices.

Maximizing Fairness

Consumers have a right to know that the data is being collected and the companies have a responsibility to minimize intrusiveness, maximize fairness, and create legitimate expectations of confidentiality. Once again, suppress notices are an important tool in making sure consumers are aware.

DMA would also suggests that the use,. and particularly the transfer, of sensitive health data be kept to a minimum; we are working hard to educate companies of that fact. But consumers must be empowered as well. Companies also have an obligation to their customers to provide them with educational information to show how they can, in fact, protect their health care data.

The survey example is a very important illustration of that point. Why did consumers tell the coupon marketer that they were on particular prescription drugs? Did consumers know how that information was going to be used? Was the suppress notice clear enough? These are all issues the industry is currently grappling with.

Physicians also should be trained to educate their customers on why the sign-up sheets exist and how the information will be used. This involves not just the confidentiality data in their medical charts, but also any type of paper trail the consumer may leave in the pursuit of health care. In the case of grocery stores, for example, some consumers truly believe that their Tylenol purchases may be considered health data. These issues must be addressed.

We should ask other hard questions at the beginning of this process. Where do we draw the line on the access, collection, and use of health data? Will it be necessary to legislate or can self-regulation fill the gap?

Many have argued that America's economic success is directly attributed to our open information society. That same tradition provides American consumers with more choice, than any other consumer in the world-not only in exercising their rights as an individual, but the choice to access valuable products and services. So far, the direct marketing industry has successfully shown the value and role of self-regulation as a customer service tool and as an alternative to restrictive legislation that may limit consumer choice. But the more we get into information management technology-into areas that are considered sensitive, like consumer health data-the more we have a responsibility, and are aware of that responsibility, to address the issues every month, every day, and respond to individual consumer concerns.

In marketing information for use by the private sector, we are trying to achieve a balance that works best for the consumers (i.e., their ability to choose), the industry and the government. I have great hopes that the dialogue we have started here today will continue and contribute to that process. As a trade association professional serving the information management industry, I look forward to continuing this dialogue. ◆◆

Health Data and the Private Sector

Stephen Brooks, M.A.
Manager, Medical Information Management
Aetna Health Plans

My perspective today is quite practical. I speak from the perspective of managing a large insurance company's health care system and of building tools to support our customers' needs and our own in-house medical and plan management staff.

The public and private sectors use health care claims and administrative data to help manage the delivery of health care and control health care costs. Insurers and managed care companies participate actively in the health care system through a provision of employee benefits, since most people receive their health care benefits through employment. The majority of those are handled by insurance companies and HMOs, although some are handled directly by employers in large cases. At Aetna, most of our business is administrative service contracts, where we process and pay claims for employers who act as the plan administrator under the Employee Retirement Income Security Act (ERISA). The kinds of information that might be shared between an administrative services only (ACS) customer who has some benefits-related need-to-know and an insurance customer who has a much more limited need-to-know differ.

At Aetna, we have managed the privacy concerns with strict policies on confidentiality and release of data. Changes in the health care industry affect how we use data but will not fundamentally alter our policies.

Ultimately we must ask: Is patient health record information really different from other personnel information in the private sector? And is the private sector unique?

An Historical Perspective

Even when I joined Aetna in 1985, capturing more than the first three digits of a diagnosis code on a claim or capturing secondary diagnosis codes on hospital and other claims was not mandatory The processor would evaluate all information on a bill in reviewing a case and in making a determination, but the information was not always entered into the system.

The information was not organized by patient, but by customer and transaction identifier. Because of the volume, the data was segmented by when we processed the claim. To build something by patient involved an enormous amount of work

Prior to 1980 on the information technology side, I use the term "big iron." Everything was main frame data processing-we began automating our old manual systems. We did not make any changes in what we did or how we did it as we built our initial automated systems. We stored all our data on cards or on tapes. When I first joined Aetna, my boss had been with Aetna since the late '70s and directed a unit which abstracted pricing data from paper claims files. The data were entered on punch cards and racks of card trays--literally hundreds of thousands of cards-and put through the pricing system. Obviously cards got damaged, and accomplishing anything was extremely difficult.

As we moved into the 1980s, the role of health care began to change. Payors became a little more proactive. We built systems like hospital precertification to assess the necessity of a particular hospitalization and to make sure that the proposed length of stay was appropriate before the claim was submitted. We built second surgical opinion programs to look at surgical necessity, In the late '80s, we developed preferred provider organizations-contractual affiliations with providers and provider groups. We began to develop the primary care physician/gatekeeper role. We began to hire a significant number of medical and nursing professional staff.

When I joined Aetna, we had fewer than half a dozen physicians on staff-we now have about a hundred. When I joined Aetna, we had about a hundred nurses-we now have several hundred. The health care professional is really altering what insurance companies do and the way they do it.

The Advent of Information Technology

In 1980s information technology, we began to see the advent of personal computing. At the same time, our main frame applications got bigger and less flexible. We moved data. from tape to disk. (In 1985, Aetna moved the AEccess system of cost and utilization data to disk It did not change the data's organization; but by moving to disk, we eliminated about a thousand tapes a year and improved-accessibility and reliability.)

The industry began to get personal computers for isolated applications and began using end-user computing. All of these applications were stovepiped, with no systematic approach towards effectively integrating information and use. Insurers and health care companies created numerous internal islands of data with no bridges.

As we move through the '90s, this situation will change. We know that our role will evolve further as we go into managed competition. Insurers and managed care companies are building stronger network-based projects (HMOs, point of service models, more aggressive PPOs, etc.). At Aetna, we expect to see a decline in fee-for-service care. Aetna's plan is to grow the managed care portion of our business over time and to shrink the traditional unmanaged care part of our business. We think that the whole industry is moving that way

Insurers and managed care companies are mainstreaming health care professionals. They are no longer isolated in a separate medical department; they are now in the field and in operational areas influencing everything we do.

The industry is getting into quality management and outcomes management. We are looking at clinical protocols, at what care should be rendered to a patient, and what is appropriate treatment We are not just accepting whatever a physician does as necessary and appropriate. Studies have shown huge variations in practice patterns nationally and these patterns are not all equally effective from a clinical or cost perspective.

The Move Toward Networking

In information technology, the industry is moving towards networking. This presents enormous problems. We will distribute data and databases; we will integrate information across different systems. We will then need to integrate data from these sources in different ways to assess quality and manage outcomes.

The market is beginning to develop more intuitive end-user computing tools. You do not need a computer programmer any more to analyze data. Physicians can actually manipulate and understand data-that is a real change.

Groupware and shared development tools are also emerging in the industry. Applications that might be developed in one area can now be distributed to other areas and shared by numerous users. Using such tools, when we find we are very successful at doing something in one part of the country, we can share that knowledge with staff in other parts of the country

The industry is also beginning to build sophisticated expert systems and decision support tools that will really help guide the clinical processes, tools which are critical in the move into network-based products. At Aetna, we are not an insurance company anymore-we are a managed care company.

What sort of data do insurers and managed care companies maintain? First, we have information on membership and enrollment. We must know who is eligible to receive payments, and what they are eligible to receive. Second, we have information on providers. We credential all providers affiliated with our managed care products. We need affiliated provider information for members to help them obtain care. We also have information on fee schedules to guide payments. We have information on our customers and their benefit plans; on the deductibles, coinsurance and plan limits; and on special provisions that might apply. We also have information on authorizations; that is, on why a physician requested prior authorization. All this is integrated with data when we process the claim. Any insurer or managed care company has a lot of data.

In comparing a claim side-by-side with a medical record, you see that a lot of information in the medical record does not go to the claim form, and not all information on the claim form is picked up by every insurer or managed care company. A core cut of data is picked up and used by most insurers and managed care companies, but not everyone uses everything.

Mention was made of Kaiser and ambulatory care data. Kaiser does not capture it, because it is not needed. The way Kaiser manages its business-with the physicians jointly responsible for care-this data has just not been critical. Other managed care companies have encountered data for capitated providers as well as payment data for non-capitated services.

The Enormity of Issues

At Aetna, we cover about 11 or 12 million people with indemnity and PPO products. We have about 1.5 to 2 million people in our HMOs and point of service plans. Overall, we cover about 13 million people, or about 5 percent of the U.S. population. Probably several of you in this room have coverage through Aetna; I do.

What kind of volume does a company like Aetna process in a day? Well, it is about noon Eastern time. We have been processing since 8 a.m. We have probably processed 100,000 claims for tens of thousands of different members. This represents about 200,000 individual medical services and will result in $25 million worth of payments so far.

In Aetna's reporting systems, the claim analysis systems on the back end of the claim process keep a few years worth of data. About half a billion services are in the system. We pay for about one million hospitalizations a year and one million outpatient surgeries. We have a fairly large database, which is quite difficult to work with. We have about 20,000 different customers, about 50,000 different plans of benefits (different deductibles or coinsurance levels), and the claim is different under each plan. This presents a real difficulty in helping our medical staff because we may not see the claim until part way through the course of treatment.

What are the traditional uses of data? Data is used for processing and paying claims, providing customer service, reporting on cost and utilization patterns customers may want, and reports on their experience subsidiary, by white collar/blue collar and by geographic area. The data is not reported by patient. We can perform benefit analysis and help plan design and management without using that level of data.

Our administrative services customers can request tapes of their claims data, which is provided with scrambled social security numbers. If they insist on getting unscrambled numbers, they must sign authorization and releases that the information will be used strictly for plan related and plan management purposes; that is our standard.

We use the data internally for financial actuarial pricing purposes to set reserves, pooling, and stop loss provisions; but again, those financial applications use aggregate data.

We also use data for fraud and abuse prevention and detection. Traditionally, we used data to assemble and develop cases and to support litigation. As we move forward, the industry is beginning to use information to assess patterns of care and to detect fraud and abuse up front. The emerging uses of health care are to develop and manage provider networks, to select providers for participation, to manage provider risk factors, to develop institutes of excellence, and to look at special provider networks for specialized services like lab and rehab.

The industry is developing programs like Aetna's Healthy Beginnings, a high-risk prenatal care intervention, to help prevent sick babies. The industry is also beginning to build patient profiles for things like drug interactions. When you go'to a drug store, the pharmacist may check your medication profile to see whether two drugs interact; if you go to two drug stores, the interaction cannot be checked. When we receive the claims, we have the information to detect those interactions. As we move to more electronic connectivity with pharmacists, we may be able to help prevent adverse interactions.

The industry is also looking at targeted risk assessments and health education. How can we help prevent people from needing acute hospitalization without helping prevent them from needing to be fixed in the first place?

What are' other uses of health care data? At least within Aetna, I am aware of none. Basically, we have very strict confidentiality policies and guidelines. If someone in another division of Aetna wanted information on health benefits, their request would be refused. That is our standard policy. Perhaps we are more stringent, but I do not think we really differ from the rest of the industry in the general use of personal data. We use the data that we have to manage health benefits. That is what our customers contract with us to do. We use it as effectively as we can. We do not go beyond that.

What we do with data is similar to what the government does (under FEHBA, Medicare, and Medicaid). They have a similar function and the same kind of data-mortality and -morbidity data, cancer registries, and other systems of disease tracking. Privacy concerns that insurers and managed care companies have are almost the same as privacy concerns of the government. Ultimately the private sector is not unique.

Where are we going from here? We in the private sector cannot solve this problem-no one company can. The nation must come up with a consensus as to what is necessary and appropriate. Industry will abide by society's decision. ◆◆

Health Data and the Private Sector-Discussion

Lorna Christie
Senior Vice President
Direct Marketing Association

Stephen Brooks, M.A.
Manager, Medical Information Management
Aetna Health Plans

■ **Participant:** Mr. Brooks, you talked earlier about how you guarded the confidentiality of information, but you also referred to yourself as an agent of the customer. What would you do if the American Civil Liberties Union (ACLU) used Aetna and said, "We would like to see individual claims data on our employees. We are concerned about how the premiums are being paid for, how claims are being used." Would you, in that situation, give the claims data? I know no legal restriction prevents your giving it, but would you give it? And if they said, "Well, if you do not give it to us, we will go to another company that will give it to us," how would you handle that?

■ **Mr. Brooks:** If it is an administrative service contract?

■ **Participant:** I do not know what that means.

■ **Mr. Brooks:** If there is no insurance, if the customer, ACLU, paid all of the money for all the benefits under that contract, then we are an administrator for the ACLU. ACLU has rights to that information. If the customer wanted it, we would provide it. We would scramble social security numbers and identifiers, unless the customer insisted that' it had a need to know individual information. The information is much like information in a corporation's personnel office. The corporation is responsible for managing that information appropriately.

■ **Participant: So, in** other words, you would give it to the ACLU and leave it to the organization to decide how it would handle it internally?

■ **Mr. Brooks: Yes,** because it is the customer's data. We are merely acting as its agent to process claims. In an area where the customer does not have expertise, we apply our expertise and systems to process and pay the claim. But the information really belongs to the ACLU.

■ **Participant:** Is there any situation where you would insist or where you would directly inform the patient, who I **realize** is not a customer of yours, in that situation? Would you require any kind of. ...

■ **Mr. Brooks:** Again, that would be the responsibility of the employer. We act as its agent as it provides that benefit to its employees; it becomes the customer's responsibility.

■ **Participant: Ms.** Christie, you have talked about the isolated incidents that occur under these new uses of health care-related data for marketing purposes. I know that voluntary **self-**regulation is a big part of the industry's privacy plan. But what do you do about those isolated incidents, other than just educating those people? Would you be willing to see a 'situation where we are not precluding individual choice and somehow always looking at a regulatory scheme to lock out an individual's ability to choose? But instead are we looking at a regulatory scheme that takes the voluntary self-regulation that you are so proud of and applies it industrywide? This would deal with those isolated incidents that you have referred to and allow a system where people have some kind of an enforceable remedy? It is not just a matter of the Direct Marketing Association coming in and saying, "Look, now that you are starting to use some of this information **for** marketing purposes, let me tell you what are some good, fair information practice principles."

■ Ms. **Chrlstle: Those** are two very important questions. With regard to the administration of the guidelines, what do we do when we find a case where a company is violating consumer privacy expectations? We actually work with the individual company I am very happy to say, in the case of **privacy** violations, we have a 100 percent compliance rate, **with** the marketer or the company stopping the practice.

I am not an expert on regulation, and I do not do regulatory work for DMA; I do the consumer affairs work. But, again, we are on record as saying health data is unique. Questions must be answered at this point in time. We need to address the issue of whether or not self-regulatory programs fill the gap or, in some situations, legislation may be necessary

■ **Partlclpant:** Well, where they work, that is wonderful. But in the situation where you try to insure compliance, the individual has no remedy The individual may not even know that a violation has occurred.

■ Ms. **Christie:** In the case you described to Mr. Brooks, would you not already have access to that data?

■ **Participant:** Not necessarily

■ Ms. **Chrlstle: These** are your employees that are participating in a benefit offered by ACLU; so would you not already have access?

■ **Partlclpant:** Well, the ACLU does not routinely get copies of claims forms.

■ Ms. **Christie:** I see.

■ **Partlclpant: I am** asking about a situation where the ACLU's premiums have gone up or it is concerned about certain employees who have taken a lot of sick leave. This is happening more and more, that the customers of the insurance companies, who are often employers, are asking for specific claims data on individuals. Many insurance companies are complying for competitive reasons.

■ Ms. **Chrlstle: Sure.** What you are addressing is the issue of privacy in the workplace. Certainly, with increased use of management technology, that is becoming more and more of an issue. That is not an area that I have any knowledge in. What DMA would look at in the legislation is the potential to make sure that what you are proposing achieves the desired purpose of giving employees privacy rights in the workplace, but at the same time does not restrict legitimate access and responsible use of that type of information. So you cannot give a generic answer to that type of question. It would have to be handled on a case- by-case basis.

■ **Participant: Thanks.**

■ **Partlclpant:** I think you have illustrated the fundamental problem of why this conference is necessary. There is a **mindset** here that somehow the payment for health care gives rights to the data. Where did that idea come from? We have a law specifically affecting students at the university. It does not matter who pays the tuition; the grades are the rights of the students. This is a bizarre, antisocial concept that you are articulating and supporting.

I am appalled. You talk about suppressing the patient's name on the prescription records. How did they get those names in the first place? I am appalled by the idea that it is a normal practice that because people must get their health insurance through their employers and because they have no alternative, that somehow the employers are entitled, because they are the customers, to their employees' data. If anything, the doctor and the doctor's representative-the insurance carriers-are **the** trustees of that data for the patient, and the employer is the precise person that the patient does not want to have that data. These are not apples.

That is why this conference is occurring. I am frankly appalled that Aetna would ever supply that data without a direct release from the patient, and I will notify my Aetna clients of that fact. I find that absolutely incredible that they would supply that data to an employer.

We have researched this in the military, where this is an internal problem. We are finding that employers are destroying employees' privacy so that they will not use the health care insurance. One of the things that you can accomplish by destroying your employee's privacy is that they do not use their insurance. It is not their money, if you will; it is a contractual obligation that they have taken on. But that does not change the ethical obligation of privacy for the patients.

As a lawyer, I am not affected by who pays my fee. My client is entitled to my fiduciary obligations. And once you get away from that concept, you have no reason at all to think of health care data-it just becomes like any other piece of marketing equipment. And the whole purpose of this is that the people out there do not accept

that. Once they know about it, they simply do not accept it.

■ **Participant:** A question to Ms. Christie regarding mailing lists. In some countries, the selling and using of mailing lists is strictly forbidden. Can you give this group your perspective of a balance between the few people who get hurt and the marketers who, for profit, continue to buy Should we not in this case look for the benefits? When we have borderline cases regarding confidentiality in many areas, then the question is need to know or improvement of procedures.

I personally have a problem seeing the benefit of any kind of activity using medical or health-related mailing lists. I believe that those countries which have clearly said that health-related mailing lists specific to one disease community should not be used in direct marketing efforts are correct in their attempt to stop usage.

■ **Ms. Christie:** I do not necessarily disagree with you. The problem with the trend in data protection regulation in Europe is that, in many cases, the legislation goes too far. Again, the Direct Marketing Association agrees that sensitive information should be treated differently In some cases, the use of that information has a limit. So we do not necessarily disagree with the concern regarding the use of specific health data information.

I would also like to make something very clear. I do not believe I said only a few people get hurt, so the problem is insignificant. Particularly in dealing with something like consumer privacy expectations—and that is one of the reasons why self-regulation works so well in this process-we do not decide what is a privacy violation. Consumers decide what is a privacy violation and exercise control in opting out and having their name removed from national mailing lists through our mail preference service.

We are in no position to judge what the individual consumer says is private, with the exception of the sensitive areas like medical data and health records. And in that case, the industry is and has always been willing to open a dialogue to discuss those issues. I cannot give you an answer.

■ **Participant:** Do you, therefore, agree that a ban would be a good thing?

■ **Ms. Christie:** I cannot tell you that, because I am not an expert in that area. I am not trying to avoid the question.

■ **Participant: Mr.** Brooks, I appreciated your comment on Raiser not including primary care information in its data system; I am not exactly sure why You also observed that most of the data that Aetna collects focus on hospitalizations, high cost procedures, and major high cost diagnostic activities that take place in the claims process. It does not apparently gather very much or retain very much data on primary care. How do you make the decision about what kind of data should or should not be collected?

Let me just follow up by saying that, at the federal level, a program called the Uniform Clinical Data Set (UCDS) gathers 1,500 data items on every hospitalization for peer review organizations (PROs); it seems like it is a fairly unlimited target for hospitalization. But in primary care, how do you decide what kind of data should or should not go into your electronic system?

■ **Mr. Brooks:** We basically take the information necessary to process a claim-the procedures, who the provider and the patient were, the principal diagnosis code, and any additional codes. We really focus on the inpatient, because this category comprises over half of our total payment costs. My recollection is that about 60 percent of the dollar Aetna pays goes to hospitals; a significant portion of the physician dollars go for inpatient hospital care. That is where most of the money is; that is where we spend most of our effort. We do have data on the outpatient care of which it becomes a part.

■ **Participant:** But my conclusion from that is that, if it does not cost very much, its value to your data system would not justify gathering additional information which might be included in a general medical record, a history, or a physical examination.

■ **Mr. Brooks:** Capturing additional information in the system is very expensive for us. We process an enormous volume of claims. Because of the volume, if we wanted to capture an additional two or three characters of information, we would need another claim processor. Every time we add a couple of fields, we increased the cost enormously. So we evaluate the cost effectiveness of any information.

■ **Participant:** How can we decide when the value of the data to be gathered justifies the additional cost and the additional risk to confidentiality?

■ **Mr. Brooks:** I believe there probably is, if computerized patient record, national data on patients, the majority of the costs, and the majority of impact on cost is evaluated. The volume of inpatient claims, of hospitalization claims, is maybe 5 percent of the total volume, representing a huge proportion of the total payments.

The reverse side is that capturing detailed ambulatory outpatient care is extremely costly. There is so much of it, and it has less value added. As we move more into managed care, we will have to evaluate the level of data.

■ **Participant:** To the last speaker, I had two strong reactions. You said we have a right to collect data. I think we need to consider that thought very carefully because data collection is a privilege more than a right. If you start from the position that it is your right, perhaps you will not be as sensitive to the other person as you should be.

And the other statement that I found interesting is that if the information is given out voluntarily, it is not sensitive. Could you elaborate on that?

■ **Ms. Christie:** As a matter of fact, I like your terminology. I generally say that the right to collect data in this country is guaranteed under the Constitution. But I also say that we must collect data responsibly and use it responsibly; so I always put two parts to the equation. I do like the way you said privilege.

Regarding what is sensitive, even though a consumer may volunteer the information, that does not necessarily mean it is not sensitive. The dilemma that I was trying to describe is how we define health data. For the consumer on a prescription drug, defining and placing restrictions on health data, such as certain types of prescription data, may in fact prevent them from exercising choice and access to other products and services.

So, again, we get back to the issue of balance. The balance is between the industry's need to access information to serve its customers, as well as to survive and to compete, and the responsibility and expectation of the consumer about how that information will be used. What we are working toward is that balance.

■ **Participant: Have** you ever done studies of how the patient or consumer defines private, sensitive, and confidential?

■ **Ms. Christie: There** are studies out there. Direct Marketing Association has never conducted a study on consumer privacy, but we certainly use existing studies to base many of the principles in the DMA guidelines, in programs such as our in-house suppress, as well as our mail and telephone preference service. The one thing you learn about studies is that consumers have parameters and areas that they consider to be more sensitive than others. That would include health records and financial information. But when you get down to the descriptions of what they mean by health data and financial information, these areas become much more difficult to define and certainly more difficult to regulate.

That is why providing consumers an opportunity to opt out right at the beginning works for American consumers; we are always trying to make it work even better.

I am not saying these programs are perfect. We are in a constant state of self-evaluation and improving the programs to make sure we are responding to the consumer privacy expectations and needs.

■ **Participant:** Do you think consumers always feel free to answer questions about medical information? Do they fear that they may not get the right treatment?

■ **Ms. Christie:** I do not know. As I said, I am not an expert in that particular area. And even if I were, it is hard for me to judge consumer privacy sensitivities or consumer fears about why they may not voluntarily want to provide information. It is an important question that needs to be addressed. I just do not have an answer for you today.

■ **Participant:** Ms. Christie, I was fascinated by your statement that you had support from the Constitution, a guarantee in the Constitution to collect data. And I would be very interested to know your basis for that statement.

■ **Ms. Christie:** I always said one day I would get in trouble for using that statement, although our lawyers say we can say that. I cannot get into a constitutional argument with you. Basically, different court cases have interpreted that marketers have the right of commercial free speech. Here is where the issue of the right comes in, but we also recognize that with that right comes a responsibility.

■ **Participant:** I am sorry, it avoids the point. Collection of data has nothing to do with free speech.

■ **Ms. Christie:** Restrictions on collection of data could prevent marketers' access to their customers. That is where the translation or the connection comes in. But I am not a constitutional lawyer. I could certainly refer you to one of the DMA counsel who could better address your question.

■ **Partlclpant: Ms. Christie,** recently I read a magazine that had a two-page, full-color spread, advertising something called Estroderm, which alleviates symptoms of menopause. They invited people to call or write in and get a free patch to try it out. I read through it twice and did not see any notification of how that information would be used or an offer to opt out of information. Should the consumer assume in that case that it will be used for a mailing list or that it would not be sold?

■ **Ms. Christie: No.** Again, you get back to the points that I address. Consumers also have to be empowered and they can certainly exercise their rights. Any time they provide information, consumers have the right and the responsibility to make sure how that information will be used. If that is done enough, then the marketer who places those ads and does not include a disclosure notice and an opportunity to opt out is not going to get responses. Here it becomes a marketplace issue and consumers have control in that area; we would certainly encourage them to continue to exercise their rights.

■ **Participant: So** the assumption is that it would become part of a mailing list.

■ **Ms. Christie:** I do not know; I am not an expert in the pharmaceutical area. My area of expertise lies more in the traditional marketers. It is safe to assume that the company is collecting that data for a reason. Either it will write to you again to say, "Well, we have developed a new product that is based on that particular product," or it will use that information to market to you at a later day, or it may exchange that information. Regardless of the circumstance, the consumer certainly has the responsibility and right to ask how the **information** will be used before volunteering personal information.

■ **Participant:** We who collect data in the government are constantly aware of a high **nonresponse** rate; because our surveys and the data are strictly voluntary, respondents may stop at any time they wish. This concerns me because a lot of the data we collect goes into policymaking decisions.

In contrast, I am afraid I am hearing that you do not have to deal with a nonresponse rate; in fact, no choice is involved. When I apply for health insurance with my employer, I am **not** given a choice as to where that data goes or how it is collected. This concerns me, and I wonder if you would address that.

■ **Ms. Christie: You are** given a choice because, in providing that information to the marketer, you certainly have the right to ask how and where that information will be used. And if you make that question part of your **purchasing** decision, then consumer privacy expectations become more important to the individual marketer. The marketer recognizes that without policies you like in the company, you go to another provider. It is as simple as that. When consumers exercise their right, it becomes a marketplace issue.

■ **Partlclpant:** But you are saying it is all dumped to the same place anyway.

■ **Ms. Christie:** Absolutely not. The marketer also has the right to respond to the marketplace demands. In this case, privacy is becoming a marketplace demand and, therefore, a customer service issue.

■ **Participant:** I want to thank Mr. Brooks for his very informative presentation of what Aetna does and does not do with personal information. I was pleased that he mentioned it has strict policies on confidentiality and data protection. I am sure you are aware that companies like American Express and Equifax have generated privacy codes that are in pamphlets and that a consumer of their services can actually see.

Does Aetna have a privacy code in accessible form that can be made available to inquiring individuals among your 13 million subscribers?

■ **Mr. Brooks:** Every Aetna employee must sign a code of conduct form; specific privacy issues are raised there. Our field office manuals for our claim processors have that. I honestly do not know whether a specific privacy issue information package is available for individual members. I will try to find that out for you.

■ **Participant:** The moral here is that if you are going to have informed consent and insure that you follow fair information practices, you should have a mechanism to inform subscribers or individual participants, especially when you are talking about **5** percent of the American population. That is the only possible way you can make self-regulation work. ◆◆

Lessons for the Future: Privacy Dimensions of Medical Record Keeping

Willis Ware, Ph.D.
Corporate Research Staff
The **RAND** Corporation

I have had a real adventure in looking back through materials that I have not read in detail for well over 10 years. I have had difficulty deciding what is important to say; so much might be. Moreover, the discussions in the conference so far have really enlarged the scope of what might be addressed.

You should not think, however, that much of what you are saying to one another at this meeting is all that new. There is an excellent body of literature on the privacy aspects of personal information databases; I trust that you all have read it. Starting with Alan Westin's *Databanks* in a Free *Society,*[1] progressing through the DHEW Committee report *Records,* Computers, and *the Rights* of *Citizens,*[2] and into the report of the Privacy Protection Study Commission's *Personal Privacy in* an *Information Society,*[3] plus other pivotal contributions, all contain much relevant material that is still valid.

Many of the expository discussions are still largely complete and accurate, and the Privacy Commission report remains the most comprehensive treatment of record keeping in the private sector.

In fact, the Department of Health and Human Services wouid do well to pull together relevant excerpts from the major documents on medical record keeping, particularly the chapter on medical record keeping of the Privacy Commission report, and republish them for the benefit of the health care community. Without much work, an additional commentary could be prepared that would bring the historical materials into the present and point out changes that have occurred (principally networking and proliferation of automated health care systems) and the consequences for earlier positions.

Having done so, I would suggest that the reprint be widely disseminated and become required reading for anyone who intends to do serious work in health care delivery mechanisms and systems. Doing something about health care is certainly on the national mind. Industry reform and reconsideration of its relationship with the federal and state government programs is high on the national agenda, driven primarily by the enormous cost of health care and the failure of the present arrangement to provide care equitably to the country's total population. The country quite clearly is going to do something; the DHHS already has a head start with its own effort to improve the payments part of the system.

I would like to consider the national mandate broadly It is time to "work the problem" instead of just talking about it. If we are going to fix the health system, then should we not throw the net widely and clean up the whole act properly, not just the part that happens to be politically important at the moment? If not now, this country may not get another chance for a long time, because the pressure for change will abate and the political noses will sniff for other issues, ones with higher social payoff, political rewards, and enhancement for the probability of re-election.

The last comment is not a critical remark about the elected people in government; it is simply a characterization of the federal government as this country has structured it and the motivations that drive it and its leaders.

Definitions

I want to deal briefly with three definitions-just to keep our discussion straight and precise. These are intended to be working definitions, not scholarly and elegant ones.

. **Confidentiality-a** status accorded to information that indicates it is sensitive for stated reasons, it must be protected, and its access controlled.

- **Information (data) privacy—a** broad term referring to the utilization, sometimes even exploitation, of information about people for various purposes. It is an information use issue, although the word is sometimes used loosely as a synonym for confidentiality or even secrecy.
- Securtty-the totality of safeguards in a computer-based information system that protects it and its information against some defined threat and limits access to the system to authorized users in accordance with an established policy. Hence, system security contributes to the assurance of confidentiality and to conformance with access restrictions and is obviously a precursor for honoring privacy restrictions.

To use all the previous terms in a single sentence: If the security safeguards in an automated system fail or are penetrated, a breach of confidentiality can occur and the privacy of data subjects invaded.

Privacy in Medical Information

Today the discussion is focused on privacy in the context of medical information. Part of the issue is included in the collateral questions: How will society permit or limit medical information use about people? How will government require by law or regulation that medical information be used?

After organizing the content of this presentation, I went back and reread "Medical Record Keeping," chapter 7 of the Privacy Protection Study Commission (PPSC) report. I did it in that sequence to avoid having my current views dominated by the earlier work. The PPSC adopted a **sectoral** approach in its examination of private sector record keeping. It studied issues one by one, and made recommendations pertinent to each. I continue to endorse that position, primarily because it seems apparent that record keeping will differ enough in detail from sector to sector that a universal position, response, and remedies **are** not likely to be possible. The PPSC material is still very pertinent, largely relevant, and **true,and** many of the recommendations are still pertinent.

Accountability

On the 1099 tax form that the Social Security Administration (SSA) sends to all who receive benefits from it, information of a privacy nature is provided. A few excerpts are pertinent today

> *Congress passed [Public Law ZOO-5031 in 1988 that says you have a right to know that we match records by computer ....*
>
> *Computer matching programs compare Social Security* ***and/or*** *Medicare records with those of other Federal, State or* ***local*** *government agencies.* ***Many*** *agencies may use matching programs* ***to find*** *or prove that a person* ***qualifies for*** *benefits paid by the Federal Government.*
>
> *You give us information about yourself. Sometimes, we check information you, and others, give us.* We use *computer matching to do the checking. The law allows us to check this way* ***even if*** **you** *do not agree to it. We may also share information about you with other government agencies that pay benefits. They will use this* ***information*** *in their computer matching programs.*

The statement happens to be worded in the **positive—"prove** that a person qualifies for benefits"-but there is an implied **obverse—** "find people who are improperly receiving benefits or are breaking the law in other ways."

Such a statement politely states that, so far as the funds that the SSA disburses are concerned, the administration is responsible for performing according to law. The SSA is to be held accountable, a construct that holds a high priority with the federal government whenever its money and/or its programs are at stake. From the government's point of view, it wishes to make sure that its funds are being used wisely for the intended programmatic purposes, and also that the funds are not subject to waste, fraud, and abuse.

In the private sector, accountability arises in a different context as a result of enforcement and/or monitoring of business practices; e.g., supervision of telephone calls routinely done by some federal agencies. This is well established in financial/business circles and a long-established practice in most service organizations that must meet the public over the telephone to monitor telephone conversations. Internal auditors have also been around for a long time and basically provide a mechanism to assure honest legally compliant conduct of corporate affairs.

Computer Matching

Any time **accountability** is a crucial item, computer matching of databases is a tool very likely to be used, and so it will be in medical **record** keep ing. Health care delivery cannot escape **account-**

ability and, at one level, it already takes place. We already have utilization reviews, fee supervision, and facility oversight.

But notice what happens in a computer match. For many reasons, some hits are incorrect. In an effort to catch the guilty, the entire population of data subjects is put at risk. The government and its agencies must be extraordinarily careful to protect the privacy and rights of the innocent. In fact, safeguards are built into the law that authorizes computer matches.

The country is now gearing up the health program to include a large new fraction of the population and is intending to revise the system in other ways. Accountability will be essential, and computer matching is bound to take place. As a lower priority item of attention, the operational effectiveness of the computer matching safeguards now in place should be reviewed. If they are thought inadequate for the health care circumstances, DHHS should seek appropriate legislative corrections.

How medical information will be required to be used in the reform of the health care system is not clear. It may perpetuate old ways or introduce new ways. Importantly, medical information cannot be allowed to be used as somebody sees fit, nor can its use be guided by practices and doctrines that have come from a different and generally non-automated paper-based past.

The Other Side of Accountability

Government money is bound to be present in health care; accountability will be a "must." The overall system is so big and involves so many people that waste, fraud, and abuse must be monitored and controlled. We have moved nationally to a mode of nondiscrimination; government oversight will be unavoidable to maintain stability of the health care system, to assure that it services are delivered with equity, and to avoid discrimination.

Well and good, but accountability is not a unilateral matter; it is very much two sided. Properly, the government will want accountability for its programs and its funds. But as health care delivery is reformed, let us be very certain that we make sure the government is accountable to the people who are served by providers and government funds.

Types of Medical Information Systems

Digress for a moment to characterize the computer-based systems in health care, and then return to this two-sided matter. It is convenient to conceptually divide medical informatics systems into three kinds:

- Systems to support operation and maintenance of a hospital, clinic, or other place in which health care is delivered. For example, logistics and supply, personnel, payroll, accounting management of accounts receivable or payable, corporate planning, cash, and investments management.
- Systems to facilitate and support the physician in his work place in the hospital or clinic. Food services, automated laboratories, pharmacies, radiology—each with its own automation and data system.
- Systems to facilitate, support, and document the interaction between physician and patient to manage the case and deliver health care. The dominant example is the clinical record.

Of course, the boundaries between these types are not rigid; data does flow among them, and sometimes the use of one kind will co-exist in the same physical computer hardware with another. Nonetheless, separating them can help us structure the problem.

Medical data is unique compared to other kinds of data about people-it has an enormously large inventory of commonly accepted usages and a large number of authorized users. Not all need access to everything in the record, and not all data is equally sensitive. Very importantly, many "users" are not bound by the professional ethics and historical customs and culture of the physician. Somehow, we must reach out through law and regulation to bind these other users to proper behavior.

Security

Because the uses of data in each kind of system will be different, the privacy issue will be more or less severe and the security problems for each different.

Regarding the first category, the hospital or clinic support systems resemble corresponding ones in business and industry; the security concerns are likely to be similar.

Physician support systems might be considered a special set of clinical data systems, although all end-users of support systems generally will not require the very broad access required in the clinical systems. Security controls must be present to limit disclosure to authorized recipients.

Clinical systems are almost certainly the most awkward for security because forecasting who will need access, where, and under what circumstances will be hard; e.g., the emergency room teams.

Privacy

With regard to privacy the major concerns pivot around such risks as personal embarrassment, social stigma, unintended discrimination, job loss, or promotion denial.

For example, the physically disabled and the mentally disadvantaged historically have been discriminated against. The country has gotten over that hump, but health care delivery offers many opportunities for discrimination to occur; for example, misuse of data about AIDS, sexually transmitted diseases, genetic aberrations, or sexual preference.

Some aspects of medical information will have major confidentiality and privacy problems until the attitudes of society change or until societal views prevail over business conduct.

Lesser but important privacy concerns include such things as

- Promotional mailings based on patient usage of drugs;
- Targeted advertising by health care providers or by medical-products producers based on events in medical encounters; and
- Use of medical information for questionable business practices such as exploitation of medical history for competitive or legal advantage.

Competition Among Providers

The pressure in health care reform is to reduce costs. Popular buzz phrases for achieving this goal include "managed care" and "competitive delivery." The implication is that providers will not have a free hand in handling a case; instead, they will have some mechanism peeking over their shoulders trying to find less expensive ways to the same end. And all of this is going to play out in an environment of competition. The health care industry already understands competition to some extent. Hospitals jockey with one another for position in a community; they do advertise. But evidently the screws are going to be rotated a few more turns, and competitiveness will get keener to bring costs down.

Just how far the health industry might go toward becoming like the rest of the business and commercial world is not clear, but it will obviously move from its present position in that direction. One must wonder how patient data might get exploited or confidentiality breached for competitive position, what corner cutting might become common, or what tricks will be invented and worked to get a larger market share.

The higher the pressure on the health industry to become more cost efficient and deliver services less expensively, the higher the risk that practices commonplace in the competitive business world will migrate into the industry delivering health care.

While we cannot pursue this topic at length, reformers should examine the risks that the health industry will unintentionally become a very different creature and that more onerous privacy issues will develop.

Some of the laws already on the books to control competitive practices, inappropriate corporate behavior, and the general conduct of business may apply to what is coming in health care. But medical information gets around probably more extensively than any other form of personal information. Already a large number of commonly accepted uses exist and a large number of people have access to it.

Should the country not get busy with the confidentiality security and privacy aspects of medical information before we force providers in the health care industry to aggressively compete? Should we not get safeguards in place before risking the consequences of competitive pressures?

To me, the response is resoundingly yes. Much of what needs to be done could well come in the form of legislation sought under the leadership of the DHHS.

A Case History

In the magazine *Details,*[4] Jared Goldstein details the activities of the Home Office Reference Laboratory (HORL) in Kansas City HORL processes blood samples for HIV. The article details how its practices were driven by the insurance indus-

try seeking to limit its exposure on AIDS. Blood samples were processed without consent forms; the computer system had no access controls, so data entry clerks commonly looked up the records of celebrities and athletes and even photocopied the laboratory, results as a sort of souvenir. Management was the typical high pressure style, demanding more keystrokes per day. Was the company driven by excessive zeal for profit or for a strong competitive position? Was the management insensitive, indifferent, possibly uninformed or poorly advised by computer consultants? One does not know, but the net effect, no matter the cause, was sloppy corporate business practices, resulting in very personal information about people leaking out and improperly accessed. We must not allow situations such as this to occur or to become commonplace, even under the pressure of a competitive environment.

Remedial Actions

We already know from past experience that medical information is disseminated widely and used in many ways-largely for purposes that have been considered legitimate only because no one has taken a stand otherwise. As we change the system, things are likely to escalate, and even more data will get around to even more places. Even more opportunities for data abuse will abound. Unless we act as a country, usages of medical information may well get out of hand and become socially distasteful. In fact, health care is going to be driven hard by competitive pressures. Unless we do all of this with great care and insight, the country could easily bumble into a system that will be unpleasant and disagreeable.

As individuals, we may not like the fact that medical information about ourselves is going to get wide use for many things, but it will be a fact of life. We will have to live with this fact to make health care delivery work equitably and at an acceptable cost. On the other hand, we would obviously need protection against the risks as personal medical data migrates around to many organizations and is handled by many people.

Confidentiality

A first order of business will be to declare by law that medical information, whether it resides in paper records or in automated systems and in whatever organization, is confidential and must be protected accordingly. The professional ethics and customs of medicine are no longer adequate because so many people are involved and not bound by them.

I would hope that any legislation passed will have such a statement. Precedent exists for such broad categorization. The 1976 Tax Act declared tax data to be confidential and the federal leverage on the states is straightforward: the state must also treat tax data as confidential and protect it; otherwise there will be no sharing.

Competitive Procurements

The government will run competitive procurements to award contracts for providers, payors, claims adjudication, and other participants in the delivery of health care. An explicit item in the bid solicitation must be consideration of the vendor's ability to specify and implement a security plan, an associated privacy assurance plan, and the required employee training program to provide relevant management oversight and monitoring. In my view, an acceptable bidder must have state-of-the-art security controls consistent with the perceived threat.

Just as the Department of Defense found that it had to investigate the software development capability of prospective vendors, so the DHHS and related federal agencies must examine the security and privacy capabilities, posture, and attitudes in prospective vendors and contractors. In fact, this probably should be a requirement for anyone who accepts federal money. Precedent also exists for broad oversight: the IRS is authorized to examine state tax-records systems and the FBI has oversight of the National Crime Information Center and its connections to local and state government law enforcement agencies. The federal leverage is obvious: behave or there will be no sharing of information and/or no federal funding.

Permitted Use of Medical Information

The government has some homework to do. Since privacy is an information use issue, the government must specify what uses of medical information are permitted and/or are socially acceptable, what general kinds of controls must be rigidly implemented, and how the government can be expected to audit compliance. Such details must also become a standard part of bid solicitation packages for providers and payors.

Authorization to Acquire Medical Data

We need to be sensitive to carrying forward procedures and practices that are based on historical

manual record systems. We need to be unusually alert to the temptation to enshrine the past in new automated environments. Many likely should be rooted out or modified to further control and limit the flow of medical information. I can think of an obvious one; namely, the blanket authorization on claims forms so often demanded of people. It amounts to a ticket for wholesale fishing, shopping, and abuse; and it certainly acts to proliferate the spread of medical data.

The practice probably stems from old insurance company habits. It may have carried over into the medical business when insurance companies became contract Medicare payors in addition to their traditional health insurance business. Some 25 years ago, the difficulty of collecting data from diverse sources by letter or telephone requests was both a deterrent to excesses and a protection to the individual.

In today's electronic era, it is entirely too easy to collect information needlessly on individuals; and once collected, it is never scrapped. The present procedure to require a blanket, usually not time-limited, authorization to seek information pretty much anywhere in the health industry puts all claimants at risk. This is because additional information is genuinely needed to adjudicate claims for a small fraction.

I find it hard to accept that the practice needs to be continued. Data would probably show that a large number of claims are successfully processed from data submitted with the claim. Moreover, with possible redesign of forms, perhaps an even larger percentage would never need an authorization. Of course, as the Kansas City example demonstrates, responsible management in medical support organizations is needed to respect a denial of authorization.

Broad authorizations to access medical information, especially in the payments process, need careful scrutiny.

The Code of Fair Information Practices

What about the Code of Fair Information Practices? Is it applicable to medical record keeping? Should or might it be imposed as a standard framework?

The answer' is both yes and no. The Fair Code stipulates that the amount of information collected shall be minimum. Medical record systems are probably not a problem. It is hard to believe that too much is collected anywhere except when blanket shopping-spree authorizations play a role, or 'when a physician might require additional testing because prior tests are difficult to acquire or get access to or as a guard against malpractice assertions.

Another stipulation of the Fair Code is the right of the patient to obtain a copy of the record. That would seem to be no problem with the administrative support systems. Usually the patient is now given or can get as much billing detail as desired. Regarding medical support systems, there is probably no harm in allowing patient access to laboratory and similar records. Some would be hard to copy-radiographs for example-in an occasional instance, something would be withheld for good cause. Some record entries will require interpretation.

Clinical records systems are less obvious. Many are still manually kept, some in a physician's own shorthand notes, and might even be in such cryptic form that even another physician would have trouble decrypting the entries. On the other hand, clinical records automation is on the up-swing, so making copies will become progressively easier and cheaper. One does not know what fraction of patients are informed enough to comprehend the complexities and concepts of clinical data. The argument always remains that some patients are emotionally or psychologically not able to hear and accept the content of a record.

On the other hand, one hears with increasing frequency and vigor that patients must be involved in their own health care. I subscribe to that view. If the medical community is serious in its position, sharing of even clinical data might become widespread.

The issue of patient access to records and getting a copy may not be an issue for DHHS to unilaterally consider. But DHHS can take the leadership in getting the provider community to address it. Perhaps a new career option is here— the medical analogue of the paralegal who can work with a patient and help with understanding.

The last part of the Fair Code deals with challenges to the record and correction of errors. For administrative systems, of course, errors must be corrected just as in any billing and charging system. For physician support and clinical systems, error correction may be an irrelevant issue generally, but a real issue occasionally Among other things, questions of legal liability may arise if a patient were to begin to

challenge laboratory results or entries in the clinical record.

The Fair Code is largely applicable to medical records, but the whole issue needs to be examined with some care and a revised Code of Fair Medical Information Practices written. This is an example of why the **sectoral** approach of the **PPSC** is appropriate. The Fair Code, as promulgated by the DHEW Committee, is not a universal magic bullet; sometimes it needs recasting and particularizing.

Data-Subject Remedies

The final aspect of the Fair Code is not really part of it, but is rather the legislative remedies that give the data subject legal standing. The situation is broader, however, because the Fair Code might not be readily imposed on **private-**sector support organizations. The question is what remedies ought to be provided by law for data subjects that can show harm as a result of improper privacy-invading use of medical information? If the country is serious about privacy in medical affairs, then the matter of legal remedies must be addressed.

More to the point though, if the people are to regain control of government and the behavior of its agencies and their contractors, then individuals must have legal tools adequate to the task of assuring that such agencies and organizations acting in their behalf are accountable and behave according to law and regulation.

The Federal Privacy Act of 1974 provides for liquidated damages and attorney fees, but it lacks the important feature of injunctive relief. For a medical privacy act, broadening the damage coverage and including an injunctive aspect seems important, but the issue is complex and needs to be sorted out with some care and diligence.

Federal agencies involved with delivering health care will be covered by whatever medical privacy provisions come into law. Contractors performing on behalf of an agency will surely be covered in the same fashion. This may even already be true. But we need some way to reach out to the private sector companies, such as in the Kansas City incident, and assure the data subject legal standing to seek redress.

Summary

Well, what have I told you? As you certainly appreciate, determining how to extend health care to all citizens, doing it equitably and affordably is a major task. The job is really much **larger—** because it will take a large information infrastructure to make the health care system work efficiently and to meet the goals of the programs that it supports.

While a lot of automated record keeping is in place today, much of it reflects old habits, customs, and practices. Some-maybe much-of it probably is not even state-of-the-art, as measured by its ability to support smooth delivery of services and an efficient payments mechanism.

I have not mentioned all of the collateral things that need to be done to put in place an adequate information infrastructure for the health care industry I have noted a few; and in each case, the task is either one for DHHS to do directly or one in which HHS should provide the leadership.

This is my list today, approximately in order of importance. Some are easy to do promptly; others require more study. Some require law; others, only regulation or agency policy. Collectively, they are aimed at bringing the dissemination of health data under control and restricted to approved uses.

- Declare medical information as confidential and protected as such; do it preemptively over state laws.
- Include privacy/security specifically in the bid-solicitation process, and if feasible and not already there, retroactively to existing contracts.
- Establish legitimate uses of categories of medical information and make these as binding as possible under contracts and by law. Provide a mechanism for reconsidering the matter from time to time, because the situation will not be static.
- Review payments arrangements that call for unlimited authorization with the view to eliminating it as completely as possible but providing an alternate means for getting additional data when required.
- Examine the attractiveness of imposing the Fair Code, and create a Code of Fair Medical Information Practices.
- Review computer-matching safeguards for possible revision,

Addendum-A Historical Note

The Origin of the Phrase "Code of Fair Information Practices"

The following reconstruction of history is based on my recollections of the time, an interchange of electronic-mail messages with John Fanning, presently with the USPHS, and correspondence with David B. H. Martin, executive director of the Secretary's (DHEW) Advisory Committee on Automated Personal Data Systems (SACAPDS). The associate executive director of SACAPDS was Carole Watts Parsons.

The so-called "HEW committee," assembled and changed by DHEW Secretary Elliot Richardson, had often met in Bethesda, Maryland, and held **meetings** at the local Holiday Inn. Occasionally, we would also use the NIH facilities at Bethesda for a meeting. The agenda would normally call for a three-day meeting and on at least two occasions, a Saturday.

On a particular occasion, we had met on a Saturday in one of the NIH buildings. Since it was out-of-hours for the building, the security guard required us to sign in individually and give our social security numbers (SSN). Committee members joked about this because we had been discussing the SSN in committee and regarded this activity by NIH as completely inappropriate. It was in winter. because everyone had street coats.

On Friday night David Martin and I discussed a set of rules, the basis for the relationship between a data subject and a record keeper. On Saturday morning, I presented the concept of a list of standard practices as a way of dealing with privacy issues and arguments supporting it as a reasonable and sensible approach. In discussing it, the committee constructed a list of what features might be on such a list.

As we thought of them, Professor Layman Allen, from the University of Michigan Law School and member of the committee, wrote them on a board. Initially, only a few entries were on the list. Computer-oriented people in the group thought of all manner of rules to assure accuracy, correction of errors, etc. One such proposal was to require the record keeper to notify all who had received personal information from it **of the correction.** We **quickly estimated** that it would be a back-breaking task for the record keeper and that it would be a superb source of income for the U.S. Postal Service.

David Martin and I left the meeting for some outside obligation. We left Layman Allen in charge. When we came back an hour or so later, the group had expanded the list to about a dozen items. By that time, it was mid-afternoon, and we adjourned the meeting and went home. David and I exchanged some private comments as we left that the list of rules had become very complex; we were both a little dismayed at what had happened.

The committee report (item 2 in the Endnotes) lists the dates of the meetings but not the places. Comparing them to calendars for 1972 and 1973, and given that the time of year was winterish, the meeting in question could have been Saturday December 16, 1972, or Saturday, March 3, 1973.

The December date is more likely to have been winterish and had only one speaker scheduled; the March date seems too late, given that the agenda for it is shown as "discussion of the final report." Keep in mind that the final report printed by the U.S. Government Printing Office was presented to (by then) Secretary Caspar Weinberger in June 1973. Thus, December 16, 1972, appears to be the day on which the committee framed the essence of a Fair Code but did not name it.

The dates of March l-3, 1973, are shown to be the seventh and final meeting of the committee, and we would certainly have had the details of the list of rules and its name settled by then. While we had no formal committee meetings between December 1972 and March 1973, we had additional drafting meetings, and David Martin, Carole Parsons, and I had a draft review meeting.

In the December-March interval, the committee not only created a full draft of the report but also boiled down to its present size the lengthy list of features from December. I believe this was primarily the work of David Martin and Carole Parsons, probably in discussions with me either by phone or in a review meeting in Washington. I do recall that David and I often had very lengthy phone conversations. We also worked out an arrangement for exchanging draft materials and comments between Washington and Santa Monica overnight. The December-March period was an intensive one of writing and rewriting.

After a drafting/review meeting, David, Carole, and I were sitting around a table in the North Building of the old HEW complex, probably on the fifth floor, which was where the committee offices were. It would have been around dinner time and other people, mostly friends of

David, drifted in and out. We were winding down after the day and chatting about various details of the report.

Someone came into the room and was introduced to me as (I believe) having worked with or was presently with the Department of Labor. The three of us had been talking about our list of protective mechanisms and, I suspect, toying with names for it.

The individual who had drifted in mused out loud to the effect: "What we're talking about is just like the Code of Fair Labor Practices." That was a pivotal comment and promptly David Martin first voiced the phrase "Code of Fair Information Practices." I believe we might have bandied about variations on the phrase—such as where to put the word "fair"-but one struck us as best and has survived.

We are uncertain about the identity of the individual who commented about the similarity to the Fair Labor Practices. It may have been John Fanning, but he believes it was not. So for the moment, the person's identity is unknown.

It is clear, however, that David Martin did coin the phrase "Code of Fair Information Practices" and that it occurred in the period between December 1972 and March 1973. Since the December event was only a week before Christmas, and drafting really got started in January, it is likely that the actual date was in February or the first part of March 1973.

Slightly ahead of the DHEW committee was the work of the Younger committee in the United Kingdom. Several other countries had study groups.

With respect to the Younger committee specifically, pages 173-174 of the report summarizes its work and lists 10 safeguards that bear some resemblance to a Fair Code; but they are much less specific and not as crisply stated as the provisions of the Fair Code. The British Computer Society had also adopted a code of ethics for its people and the Younger report supported and adopted it also. There is no mention of the term "Fair Code" or even of a code in the summary of the Younger report. In fact, we used its own phrase "safeguards." Had the Younger group used the phrase Fair Code or even code, I feel certain that we would have acknowledged it and also used it in our report. Thus, Code of Fair Information Practices appears to be uniquely American and to have been originated by David B. H. Martin.

Endnotes

1. Alan Westin and Michael Baker. 1972. Databanks in a Free Society. Quadrangle Press.
2. Records, Computers, and the Rights of Citizens. July 1973. Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education and Welfare, (OS)73-94. Contains a good bibliography.
3. Personal Privacy in an Information Society. July 1977. Report of the Privacy Protection Study Commission. There are also five appendices on specialized topics, including a discussion of how the 1974 Privacy Act had been working.
4. Jared Goldstein. "Blood Money" Details, November 1991, pp. 92-95. ◆◆

Research Use of Health Records: The Individual's Contribution to Medical Knowledge

David Pryor, M.D.
Associate Professor of Medicine
Duke University Medical Center

An optimist is described in a story about a father and his five-year-old twin sons. One son was an optimist; one was a pessimist. One day the father said to his wife, "I am a little worried. I think our pessimist is going to do fine in life-he will not be too disappointed. But I am not sure the optimist is going to do okay. I think we need to do something about it."

At Christmas time he said to his five-year-old son, "I want to give you your Christmas present, Son." The father took the child out to the barn on their farm, handed the little boy a shovel, and pointed to a pile of horse manure. "There it is," said the father. The little boy looked up, said, "Thank you," and started shoveling away, quite happy and pleased. The perplexed father said, "I'll come back in a couple of hours and see how you are doing."

After a few hours the father returned. The little boy was still happy and singing and smiling. The father said, "Son, I don't understand this. This is your fifth Christmas, one you are going to remember for a long time, and all you have gotten is a pile of manure and a shovel. How can you be happy and smiling and singing?" The little boy looked up at his father and said, "Daddy, with all this manure, there must be a pony somewhere."

I am often referred to, particularly by the people I work with, as an optimist. While we see a lot of potential problems as we begin to look at information and access to information, I hope we will not forget what some of the advantages are as we begin to combine information. I have been asked to represent the research perspective. I will focus on several different sections, not in great detail, but I will try to give you a taste of why I think health records are so important.

Observational Versus Clinical Data

Marked differences exist between observational data and clinical trial data. Randomized clinical trials are clearly the best approach for determining efficacy of a particular procedure. Randomized trials tend to focus on subsets of patients, whereas observational data potentially focus on all patients. Cardiovascular disease has probably been more extensively studied than any other disease; as a cardiologist, my examples will be drawn from that area.

Clinical trials use prospective data collection. Observational data is collected in many ways-it can be prospective, abstracted from charts, collected from. other forms, or collected as a by-product of other processes, such as administrative claims billing.

Observational data records a continuous experience, whereas clinical trial data records experience for a finite period of time. Clinical trial data is necessarily distinct and separate from the patient care process, and an added expense. Observational data, while it may have some elements that are distinct from a traditional clinical care process, is at least potentially cheaper. Clinical trials often define the value of a given therapy performed in ideal settings, or the efficacy of the therapy

Observational data helps us to understand the value of therapies as they actually occur and are applied to the real world community They provide us with a much broader perspective. Observational data also makes possible, because of long time periods, understanding of how the natural history of diseases, as well as therapies used to treat those diseases, have changed over time. For example, our appreciation of the value of bypass surgery for patients with coronary artery disease has changed since we recognized improvements in therapy over time.

As we look at specific health information about individual patients, we want to know whether or not we can combine that data with outcome data to make outcome predictions and use that information to help the current management or policy decisionmaking of patients.

Soaring Costs and Variability

According to the New York Ties this year, health care is up to 14 percent of the gross domestic product, and the cost is soaring. Now, combined with that soaring cost of health care is the substantial variability in this country of practice and outcomes for individual patients. In one classic study referred to as small areas analysis or small areas research, large aggregate population groups were collected. In this study conducted by Mark Chasen and his colleagues at the RAND Corporation, researchers used the Medicare Part B claims data from the 13 sites that were constructed--one in Arkansas, Colorado, and Iowa; two in Massachusetts; one in Montana; three in Pennsylvania; one in South Carolina; and three in Northern California. Now, these were large population areas.

We can see no reason why one large area of Northern California ought to be inherently different from another. We expect similar rates of underlying disease and disease severity within the populations. If patients were treated in uniform fashions, we would expect similar outcomes for patients and similar frequencies of procedures performed. The researchers computed the statistics for 123 different procedures across these large population bases.

Researchers found tremendous variability in the use of procedures and other studies of demonstrated end outcomes across the country. For coronary artery disease, for example, they divided all 123 procedures into three groups-those with the greatest variation, those with the least variation, and a middle group. They found that the use of coronary artery bypass grafting per 10,000 eligible beneficiaries ranged from a low of 7 per 10,000 to a high of 23. This is more than a threefold variation. They found a two-and-a-half fold variation in cardiac catheterization.

Most studies document this. This is not a new phenomena. The first reference I found actually referred to the Glover phenomena. Glover, a physician in England, found that the rate of tonsillectomies performed per 10,000 children varied dramatically The first report was in 1939, and the only variable that seemed to correlate with the variation was the physician's belief in the procedure.

Cost Versus Value

When you focus on costs, the goal is to reduce expenditures. When you focus on value, the goal is to get the most for the health care dollar. Most of the revolutionary changes in how we delivered health care in the '70s and '80s were, in fact, focused on trying to reduce cost. I hope that as we move into the '90s and beyond we will focus on value and how to get the most for the health care dollar. Health care value focuses on the outcome achieved for the money spent-the marriage of cost and effectiveness then becomes critical. The assessment of the effectiveness component may require the use of specific health care information.

Another type of observational database, drawing from our own experience, is the Duke database for cardiovascular disease. The Duke database was started in 1971 with retrospective data collection to 1969. The concept was to use the computer as a memory expander so that all patients would be characterized at baseline. We replaced the doctor's dictaphone with a form and the secretary's typewriter with a terminal, and automatically produced the reports of the patient care process directly from the computer files. We followed all patients routinely for regular and specific outcomes at regular intervals to be able to use the computer as a memory expander. This was a way of trying to link the process of patient care to an outcome of patient experiences.

One study, a large group effort, involved a population of 5,809 patients who had their first catheterization between 1969 and 1985. For perspective, the Duke database now prints out some 60,008 to 70,000 patient care reports a year of 50 different types. We currently follow 25,080 patients on approximately 17 different protocols. These patients were not randomly assigned to medicine or surgery they were just followed as part of their patient care process, and the follow-up was better than 98 percent complete.

Because this is not a randomized trial, patients are treated with therapies that their physicians feel are beneficial for them. To control for differences between baseline severities for patients, we used a Cox Proportional Hazards Model. For the biostatistically inclined group in the audience, we actually wrote the model for SAS as a result of our analysis needs.

Characteristics Predicting Outcomes

We spent a long time trying to understand how to estimate outcomes for patients with coronary disease. We have investigated a number of different methodologies for making predictions and a number of methods for assessing the quality of predictions and for determining their generalizability. This results in a whole series of characteristics related to outcomes for patients with coronary disease. These characteristics help us predict how long a patient will live or the survival rate of a patient with coronary disease. They include things like the underlying ventricular function or ejection fraction, the patient's coronary anatomy, and the degree of myocardial damage that is an index represented by several characteristics. We combine these characteristics to produce an outcome prediction for each patient, which we can then apply to a new group of patients.

The first part of the study consisted of an independent group of over a thousand patients. For each patient we used the characteristics to make a two-year survival estimate. We then grouped those patients, based on their two-year predicted survival, into 10 different groups. One group, for example, had a two-year predicted survival probability of about 51 percent; in fact, at the end of two years, 55 percent were alive. Another group had a two-year predicted survival of nearly 100 percent; at the end of two years, nearly 100 percent were alive.

Success of Outcome Predictions

We have also looked to see whether or not those outcome predictions developed from this observational clinical database compare to the randomized trial results. Of those patients eligible for the European Cooperative Surgery Study, we considered these questions: If we were to estimate their survival at the end of five years, how many would be alive in five years if treated medically? How many would be alive in five years if treated surgically? What was actually found in the randomized trial itself?

The most rigorous test of an outcome prediction for Star Trek fans would be to move the model across space and time. In this case, we moved an outcome prediction set into a new population of patients where the management practices were radically different from the management practices that might reflect bias in how a patient would get into a sample or institution. In fact, we found in Warsaw, Poland, in a consecutive series of patients treated in one of two ischemic heart disease clinics, a dramatic variation in population differences across a wide variety of characteristics.

The model's test is whether or not it can be adjusted for those differences to predict outcomes well. When we estimated what we should see for patients, and we compared it with what was actually observed over a period of five years, it was nearly identical. I hope I have convinced you that you can, in fact, make an outcome prediction.

Another study we did was to compare how well that prediction does compared to the current method. We asked our senior cardiologists at Duke to make outcome predictions with the question: "If we predict outcomes and you predict outcomes for the patient, who does better?" We found that even though our best doctors did quite well, the use of accumulated institutional experience contributed significantly to what is potentially possible in making outcome predictions for patients.

The value of outcome predictions has to do with their ability to both quantify variability for their use in empiric profiling, for their assessment in trends, for the use in global planning, and for how they might be integrated in value into health care. In the interests of time, I will skip over how you would actually pull together an idealized value curve, but we can actually construct a marginal value curve based on empirical data and then integrate that routinely into the practice of clinical care.

Patient identifiers are required for a number of studies, for example, to assess data quality, to link with other. data sources, and to construct a longitudinal record. In a current study, we are trying to aggregate or estimate costs from charges and the ability to go to individual records. To understand how to do that, where we have access to a records system, gives us a handle on trying to understand how to interpret large datasets, such as the Medicare dataset.

The confidentiality safeguards need to be in place. Before we were able to look at the Medicare data, for example, we had to sign a global policy statement form that I refer to as "my first born form." This gives you an indication of the significance of that form. Part of that was to review individual plans. On the Duke database, we have a whole host of characteristics that are designed to ensure confidentiality. The data is not residing on a public machine and there are no guest accounts; the patient I.D. is recoded; the

I.D. in the sequence I.D. is an encrypted file; accessing the file requires an encryption key known to only two people. The file itself will be removed from the system when all the tapes are put together. The original tapes are stored in a locked and secure fireproof vault. We have passwords for machine and file area, and no listed programs; forms are signed and paper routinely must be shredded. We have instituted a whole series of safeguards to handle the information.

Conclusion

Observational data offers unique strengths. Outcomes can be predicted. Policy and patient decisions improve when based on empirical data. Patient identifiers are necessary for some applications, and methods are available to help protect the identity of individual patients.

I would like to close with this quote:

> *That it will ever come into general use, notwithstanding its value, is extremely doubtful because beneficial application requires much time and gives a good bit of trouble to both patient and practitioner because ifs hue and character are foreign to all our* habits *and* applications.

I think you could use that quote to refer to what we have been talking about today. The quote, however, is from the London limes in 1834 and refers to ... the stethoscope. ◆◆

Research Use of Health Records: Social Needs and Personal Privacy and Research- Aggregate Databases

Dale N. Schumacher, M.D., M.Ed., M.P.H.
President and CEO
Rockburn Institute and Commission on Professional and Hospital Activities

Introduction

About a year ago, I attended another AHCPR conference in Atlanta where we discussed effectiveness of ambulatory care data. During that conference, my data privacy needs were breached. Someone entered my hotel room, appropriated my backup phone charge card number, and ran up an $18,000 phone bill. I am very sensitive to the issues of intrusion and privacy

At the same time, I am a strong advocate of the use of data. I take the position that healthcare providers are best positioned to provide the balance between citizen privacy and use of data for research purposes and the public good. I speak from a private-sector, provider-oriented approach and as senior medical advisor to the Commission on Professional and Hospital Activities (CPHA). CPHA is sponsored by the American College of Physicians (ACP), the American College of Surgeons (ACS), and the American Hospital Association (AHA), so I have particular biases that support the provider perspective. Additionally, Rockburn Institute, my home institution, has a board which consists of all providers or researchers.

Explicit Guideline&

Let us begin by considering what Ruth Faden questioned in the keynote address: How explicit are the promises, how clear are the directions? This hearkens back to London during World War II with the following directions:

> *Caution. The bombs in this crate are packed in a different manner than that formerly used. Compared with the old method, the bombs are now packed upside-down and the crate must therefore be opened at the bottom. To prevent confusion, the bottom has been labeled "top."*

Do we have as explicit directions that come from the provider community regarding use of data? The answer is yes. The AI-IA issued a 1990 Information Management Advisory' position regarding internal use of data that stated, "access should be provided only on a need-to-know basis." While we may disagree about who has the need to know, the list of those who might have a need to know is very substantial.

The same advisory speaks to external use. It reads, "No hospital should disclose medical record information to a third party without the patient's written authorization unless such disclosure is permitted by the hospital under certain circumstances for research activities, provision for state vital statistics laws," and so on. The advisory suggests that the hospital's chief executive officer (CEO) should determine whether or not to permit medical records maintained by the hospital to be used by a third party, unless the project's purpose outweighs the nominal risk to the patient's privacy rights. The CEO should have this authority clearly delegated from the board of the hospital, which is made up of the public representatives from the community so these decisions would be derived from their guidance.

The AHA advisory provides other guidelines. The proposed methodology should not violate limitations placed on the medical record information. The advisory requires that safeguards should be adequate and a log be kept of all disclosures to third parties. We are going to be faced with an increasing number of problems with the extended use of distributed databases about how we track whether particular files

have been accessed. This is a technology problem that needs to be solved.

Regarding the physician perspective, the following ACP[2] ethics statement was published December 1992: "The physician must not release information without the patient's consent unless required by law or if there is a duty to warn." At the same time, this confidentiality is not an absolute prohibition. It may have to be overridden to protect others or the public. ACP also states that decisions concerning resource allocation must not be made for the individual patient but needs to be balanced for overall societal needs.

The CPHA Research Experience

CPHA has worked with hospitals and researchers for more than 35 years and has not had serious confidentiality or security breaches. Recognizing the rights of the hospital, its confidential information, and its business services, CPHA agrees in its contract with the hospital to keep such information confidential, to protect the client's proprietary data information, and to prevent the disclosure to third parties.

The agreements that CPHA fashions with hospitals and with the providers can be unique to that institution's needs, and it can sometimes take up to *six months* to achieve an agreement as to how the data might be used for research projects. Hospitals usually identify the doctor and patient by code numbers, the meanings of which are generally not known to CPHA. Some hospitals are flexible on this, some are very rigorous and complex in their encryption, and others fall somewhere in between. The hospital generally grants to CPHA the use of the data for statistical analyses and applied research that are somewhat akin to, although not as sophisticated as, random clinical trials.

CPHA is the owner of the database generated by participating hospitals' submitted data. For example, the National Association of Children's Hospitals and Related Institutions (NACHRI) has an agreement so that as owner of the database, CPHA may access it for research, education, and database activities. Again, the individual hospital can say, "You cannot use records for a specific purpose." Providers have considerable experience in this area and have encouraged the use of aggregate databases for a variety of beneficial purposes.

Something CPHA commonly does is mask and mix the data. From the agreement with NACHRI, such data submitted shall be identified as originating from specific hospitals and cannot be use without being mixed with a significant body of other pediatric data. CPHA has another major agreement where it looks at very detailed process-of-care data, and it cannot use that data for certain analyses unless at least 50 percent of the data is from hospitals other than those under this major agreement. That is, 51 percent of the data for analysis must come from other hospital systems. This is a useful and convenient way of masking and guarding provider confidentiality

A Framework for Database Oversight

To further the appropriate use of aggregate data, I suggest a particular approach for handling these databases.

The issue that confronts us is cost containment. We are currently spending about $1.5 million per minute on health care. Since we started this conference this morning, we have spent close to $650 million on health care. We have an issue that will not go away; we are going to have to deal with costs. Cost containment will be more important than access or outcome.[3] We can segment these databases in ways that we can deal with the cost question, which is primarily a process issue,[4] without the complex privacy issues that relate to long-term outcomes.

The question is this: how might we organize our databases? We must consider organizational arrangements for databases and think about a resource management alliance and a provider-led clinical analysis. To achieve this, we need a governance board, we need a staff, and we clearly need a research capacity. To support this, I propose a bicameral database. We need one database that is primarily resource monitoring and management and another database that supports more detailed clinical analyses. These two databases will require different levels of security In reality, there would be a large number of databases with varying levels of security.

The governance board is the most important component of this approach. This needs to be established immediately, with representation by physicians, hospital administrators, nurses, and the public. These organizations need to be established community-wide or regionally The governance issues are substantial: linkages, data quality security, and confidentiality. A traditional governance setting is most appropriate for these responsibilities.

Staff is also a very important area. Those of us in the health care arena are intensively profes-

sionalized regarding the privacy of the doctor-patient relationship. At the same time, programmers and systems analysts go from one industry to another. We need to work very hard with data analysts who may have come from a direct marketing agency a meatpacking company or a communications company before becoming programmers in an institution that deals with sensitive health care data. Culturation of the nonhealth provider staff is critical.

The research component offers great opportunities. The closer that we can get the researchers to the day-to-day process-of-care, not only in the outstanding academic institutions but also in community hospitals, the more society will benefit. The community hospitals will benefit by working with researchers,, and the researchers will benefit by having access to data.

The first of the bicameral databases is the resource monitoring database. This database could contain UHDDS (Uniform Hospital Discharge Data Set) data, limited outcome data, performance indicators, and resource-use data for federal and state budgets. Insurance claims data should be linked to these data eventually on a real-time basis.

The second of the bicameral databases is the detailed clinical analysis database. Access to this detailed clinical performance data through a systematic process with specified professional involvement[5] will encourage a greater willingness to share data, use it for benchmarking purposes, and even produce "report cards." This would be in marked contrast to the suspicion and delays that occur when such activities are the responsibility of state or federal governments. At the same time, the public has the right to expect the highest levels of performance from health care providers and practitioners and should provide detailed oversight to these professionals.[6]

In summary the private health care sector already has substantial experience working with confidential data. This is a strength that should be a basis for building expanded linkages and responsibilities. Research procedures, linkages, and safeguards already exist.' The need for a unique patient identifier is excruciatingly essential. My encrypted social security number is XXX XX XXXX. It is crying out to be used by health care providers. Put it into a database and use my health care experience for overall societal good.

Provider-dominated, private/ public information alliances are the next step.

Endnotes

1. American Hospital Association. 1990. Disclosure of Medical Record Information. American College of Physicians, Chicago.
2. American College of Physicians. American College of Physicians Ethics Manual. Annals of Internal Medicine, 117(1 December 1992): 947-60.
3. Aaron, H.J. 1991. Serious and Unstable Condition: Financing America's Health Care. The Bookings Institution, Washington, DC.
4. Schumacher, D.N. The Effective Language for Quality Assurance. *In* Cornerstones of Health Care in the Nineties: Forging a Framework of Excellence. Proc. National Conference on the Quality of Health Care in the U.S. September 16-18, 1990. JCAHO, 1990: 89-97, Hot Springs, VA.
5. Schumacher, D.N. Organizing for Quality Competition—The Coming Paradigm Shift, Frontiers of Health Services Management. Spring 1989: 4-30.
6. Benvenlste, G. 1987. Professionalizing the Organization. Jossey-Bass, San Francisco.
7. Pryor, D. Research Use of Health Records: The Individual's Contribution to Medical Knowledge. Presented at Health Records: Social Needs and Personal Privacy, sponsored by the Task Force on Privacy. February 11, 1993. Dep. Health Human Serv., Washington, DC. ◆◆

The author would like to thank J. Graham Atkinson, Ph.D., for his suggestions and refinements regarding the Clinical Analysis and Resource Management Alliance.

Research Use of Health Records-Discussion

David Pryor, M.D.
Associate Professor of Medicine
Duke University Medical Center

Dale N. Schumacher, M.D., M.Ed., M.P.H.
President and CEO
Rockburn Institute and Commission on Professional and Hospital Activities

■ **Participant:** Given the countless examples of using data-electronic and computerized-in evaluating hospitalized and perhaps many other patients receiving major procedures that can justify cost savings, cost improvements, or improvements of process, how do we measure where we cut that off? Is there a place to cut that off in developing such data systems in the primary care setting? How can we determine how to make a worthwhile investment in a complete patient-data record for the full range of health care problems or nonproblems that present themselves in physicians' offices?

■ Dr. Schumacher: It is certainly difficult to measure. I take the very utilitarian or pragmatic view that we ought to draw on the databases that exist and not get into additional data collection or do so only in selected situations. So as a byproduct of the care process, we should capture the data, making the cost of capture very minimal.

This is challenging and difficult in an ambulatory setting. When we started the PSRO program 20 years ago, gathering the simplest data gave us enormous headaches. Insurance industry representatives talked about three digit codes. But some people were using ICD-7 and 8 and others were using different coding systems.

We have an $800 billion industry out there that needs this data to provide services. We need to create trust in whatever umbrellas are available to access parts of the data accumulated in the care process, so the cost will drop over time.

■ Dr. **Pryor:** Whenever we do a cost study, we always ask two questions up front: Whose cost are we talking about? And what kinds of costs are we talking about? Are we talking about direct costs or indirect costs? Are we talking about marginal costs only? Much of the record cost expense may or may not be related to additional costs, and a lot of cost is not really at the margin.

As health care providers, we **are** collecting and storing information in inefficient ways. In fact, you could argue that we could routinely record that information in a standardized way and not add too much **more** at the margin. If linking data has value, how efficient and easy is it, and what is the infrastructure for doing it? This can be approached in a **stepwise** fashion. Therefore, we could think about doing it.

Any studies that focus on limited subsets of the population will give us an inkling about what is going on with people who get that type of care. But these studies will not inform us about whether people are getting care or about some of the important access problems that must start at the primary care level.

■ Participant: Assuming a marginal cost, are we obliged to do an assessment of marginal costs and the risk to confidentiality before we jump into a patient data statement, rather than demonstrating that it has a value before we make that investment?

■ Dr. **Pryor:** The likelihood that we could answer all questions that would arise is small. We would probably be better served by focusing on some of the areas. But I am a little bit like Nike Noah, too. I think we ought to just do it.

■ Participant: Dr. Schumacher, about the suggestion for a unique patient identifier, I have heard that repeatedly from people in the health

care sector, and I agree with that requirement. But I think you are pushing a chain when you try to link it to the social security number. As soon as you do that, you are dead in the water, and I wondered why you did that?

■ **Dr. Schumacher:** Partly to engender discussion, but the idea is there. I am told by experts on security-Department of Defense and CIA types-that one can encrypt data very well. If indeed one can encrypt data to guard confidentiality, the question is not whether to use the social security number, but about who holds the keys for encryption. That is why the governance of these clinical analysis resource monitoring information alliances becomes so important.

If we did a poll in this room, most would not vote to have their social security number encrypted. But we must move quickly. I would rather take a chance in the short run and do the social security number encrypting than wait two or three years. We have been talking about this for years-let us either do it or not. I am in favor of that because I think it would offer society the most utility.

■ **Dr. Pryor:** I believe that last year the Health Care Financing Administration (HCFA) mandated the use of the social security number through legislation.

■ **Participant:** It was a bill. The Bush Administration sent a bill to Congress called the Health Information Reform Act, or something comparable. It would require all financing data to be converted into electronic form by September 1993 and begin to convert hospital information for Medicare-patients. It specified that the social security number would become the unique identifier. The point is that it has been very seriously considered as a unique identifier. I am not trying to draw judgments as to whether it should or should not be used, but proposing it is not a pie-in-the-sky idea. It has been proposed in a bill that went forward to Congress last summer.

■ **Participant:** Regarding a previous question on ambulatory care data, David Pryor's presentation discussed routinely using secondary data; that is, observational studies on data collected. One of the major uses of that, of course, is outcome studies. It is virtually impossible to really affect the outcome studies based only on inpatient data. In almost all cases, the ambulatory setting needs a combination with good follow-up data. In many cases, that is in the primary setting, once the patient has been discharged from the hospital.

We should develop some sort of uniform ambulatory data set that can be combined if we are to use these types of studies in a really radical and appropriate way. At the very least, I would not demean the importance of ambulatory data or primary data to such a degree. I would caution against prohibiting its use on the basis of confidentiality issues; this is the wrong way to go.

Once you develop an ambulatory uniform set, it is not cost effective to determine what to leave in or omit. It probably is more cost effective to routinely collect as much as you can, rather than going down the road and finding that your system had not collected what you ultimately need for study.

■ **Dr. Pryor:** Agreed.

■ **Dr. Schumacher:** Agree.

■ **Participant:** First of all, congratulations. At a recent meeting of the World Health Organization, someone stated that the first commandment of any researcher is to ask for as much information and in any unrestricted way You have achieved that in your statements. But must we have patient identification in an unrestricted form? I would like to see some documentation on that. A number of people say the differences are minimal.

The next point to consider is how we are dealing with the existing databases, such as the database in Lexington, which is being exchanged with Harvard University. Some outsiders from Europe are paying $100,000 a shot to get one search of that database. How can we come up with some way of organizing these databases? And why do we need the patient identification?

■ **Dr. Schumacher:** I would reemphasize the governance of these information alliances. One may conceivably say that the State of Maryland or the Baltimore-Washington Corridor Information Alliance does not need patient identifiers. While U.S. policy is desirable, we do not have the same social contract between the people and the federal government that exists in several European countries. The United States has, as the French say, the middle associations or middle government, whereas France has a much tighter social contract.

We must draw on the heterogeneity of our society, our states, and our various socioeconomic areas. Indeed, some may choose not to collect

particular types of data. That is why I think a budget cap becomes very important, because we must say to the community "If you have X dollars to provide health care, you have got to make some very tough decisions." And the governance unit can say, "We are concerned about patient privacy. We do not want to collect these data elements." Then you live with the financial consequences, which may be a very good decision.

That is the way we conduct natural studies here in the United States, by getting several demonstrations going or giving the states some flexibility.

■ Dr. **Pryor:** Your question had two parts-the first is why we need identifiers and the second was the state of existing databases. Let me combine those into one answer.

As part of the Port Grant supported by the Agency for Health Care Policy and Research and Ischemic Heart Disease, we are linking 18 separate databases from the United States and Canada. Those databases include the California Discharge Abstract Database, the Manitoba databases, four to six separate Minnesota heart databases, the Northern New England database, the New York State databases, both the clinical and the Sparks data sets, HCFA, Medicare databases, the Duke cardiovascular databases, the Durham VA databases, and several other data sets. These are all being linked to provide and pull together our best sources of information about patients with this disease. This is so we can develop state-of-the-art decisionmaking to underlie decisionmaking and policymaking for patients with the largest consumer dollars, procedures, and deaths in the United States. That is the goal of the project.

A whole range of information is in each of those data sets. They range from very, very detailed databases-like the Duke database-to very, very small population subsets-those populations of patients coming to Duke-to very, very large databases-like the Medicare database with its current limited clinical information of uncertain quality.

How do you link that information across different databases? The ideal would be one super set of reliable information about all patients. One way to approach the problem is to understand the quality of the data in the different data sets. As part of the work for our Port Grant, we have done a series of four separate studies linking databases to understand the information quality of the data sets and how to apply them in a larger context.

When we link to the California database, we can only go so far. We do not have patient identifiers available as part of the California system. This limits durability to examine specific elements of data quality.

We can, however, ask, "If we collect this information clinically, how often is it actually recorded in a database?" We have linked different subsets of information; for example, the administrative data record that would be sent to HCFA as part of the Medicare database with the actual prospectively collected clinical data from Duke.

The Duke data do not improve because we have collected them prospectively; but they do considerably inform us about how to apply the elements in the much larger database. We begin to approach some of the outcome issues for the country and the Medicare databases.

In the same way we need to look at charges and costs. We have potential charges and charge-to-cost ratios that are part of the Medicare data. These lack the uniformity-for example, in how different categories get aggregated across costs and charges-to link up some of the financial pieces. So we do have the opportunity to understand the quality and the ability of the data.

Suppose we wanted to understand if we can use Medicare better. Instead of the five comorbid condition limit, we could link people to the previous year data and establish the linkage. Maybe the only important comorbid conditions are those that required hospitalization within the last two, three, or four years. But to do that, we need a way to go across records, either across databases or with identifiers within a particular database.

■ Participant: One final question. It seems to me that AHCPR is quite involved in that. Do you think the agency will in the near future come up with some regulations?

■ Participant: Well, I cannot really speak to that. The most important part of that is the alliance on governance that Dr. Schumacher suggested. This is not a one-sided Agency for Health Care Policy and Research (AHCPR), federal government, or public sector issue. The issue is how to develop some shared vision at the top. And I do not know, offhand, a step-by-step procedure for developing it, but I think that would be necessary to get a truly acceptable working governing board to do what needs to be done and protect privacy at the same time. ◆◆

Administrative Uses of Health Records: Monitoring, Government Systems, and Law Enforcement

Janis Curtis, M.S.P.H.
Assistant Vice President for Special Services
Duke University

You may be wondering why **someone from** Duke University Medical Center is here speaking about uses of health data in government. Prior to joining the staff at Duke a little over a year ago, for six years I was the executive director of the North Carolina Medical Database Commission. The commission is North Carolina's state data organization. It is responsible for collecting hospital discharge data from over 150 hospitals, for building a hospital discharge database, and for routinely distributing information in aggregate form about hospital charges and public utilization. It is within the context of my experience with that state agency that I offer my comments.

Currently, the country has almost 40 state health data organizations. All of them maintain statewide hospital discharge databases; some also maintain databases containing hospital financial information and information about nursing homes. A few collect ambulatory care data. These organizations **are** literal gold mines of health information. Consequently, confidentiality and appropriate use of the information collected are serious concerns to the administrators of these organizations.

It is important to emphasize the difference between a medical record and a health data record. State agencies typically do not have actual medical records-that is, the types of records maintained by **hospitals,** doctors' offices, and clinics-that contain the patient's medical history lab results, doctor's notes, and other information.

For the most part, state agency databases have data records that contain some medical information, usually diagnoses and procedures performed. Several different types of data records containing health information are collected routinely Examples of these health data records include

- Hospital discharge records;
- Vital statistical records, that is, birth certificates, death certificates;
- Records maintained in various disease registries, for example, cancer registries, birth defects registries, genetic disease registries; and
- Medicaid paid claim records.

Some of these records have patient name and address; others do not. This variation is usually the result of the reporting requirements of the collecting agency. All state agencies, even within the same state, do not collect and maintain the same level of patient identifying information.

Medical Database Commission

The Medical Database Commission in North Carolina collects data for every patient discharged from a hospital, including self-pay, indigent, and charity patients. For each. patient, hospitals are required to submit a data record with about 21 data elements abstracted from the UB-82 claim form. The database includes

Patient information

- Age (calculated from date of birth and admit date)
- Sex
- Social security number
- Zip code

Utilization information

- The number of days for the hospital stay (calculated from admit and *discharge dates)

Clinical Information

- Patient's primary diagnosis and four secondary diagnoses
- Procedures performed

Charge Information

- Total charges
- Charges for service categories

Provider Information

- Identification of the hospital
- Identification of the physician (UPIN)

Primary **payor** Information

- Identification of the party responsible for paying the hospital bill

This is the type of hospital discharge data collected by most state data organizations, with a few notable exceptions. In North Carolina, we collect the social security number as well as the physician identifier. The commission collects inpatient data from all hospitals in the state, including state and private psychiatric hospitals. Although the health data record maintained by the commission includes patient social security numbers, the commission does not collect patient names; nor does it have a table for cross-referencing the social security number with a name. Thus, the commission cannot *directly* identify the patient from the information housed in the database.

Unfortunately, we do not collect patient race, a very important variable, given the disparity in health status among different racial groups.

For fiscal year 1992, the North Carolina database has over 870,000 data records; the commission has at least three years worth of hospital discharge data. State data organizations, like the North Carolina Medical Database Commission, are tremendous resources for health data. And their primary mandate is to provide health data to the public to aid decisionmaking about health care. I think from this profile, you can see why I stated earlier that state data organization administrators are very concerned about data confidentiality and about appropriate data use. They are constantly engaged in a balancing act to protect confidentiality, on the one hand, and promoting widespread use for research and decisionmaking on the other.

Uses of Hospital Discharge Data

State government consists of a number of different agencies, offices, and commissions. Some of them collect and/or use health data for various reasons. The following list illustrates the variety of state agencies that use aggregate health data:

- Medicaid program
- Public health director and managers of public health programs, e.g., maternal and child health programs, diabetes management
- Insurance department
- Center for health statistics
- State data organization
- Health planning office
- State Employees' Health Plan

In addition, the legislature and its staff as well as the staff in the Governor's office use data.

But simply identifying the various agencies, offices, and commissions is not sufficient for our purposes this afternoon. We must also consider the responsibilities and duties relating to health care with which government is charged. State government is a

- Payor of health care services;
- Provider of care;
- Policymaker; and
- Regulator.

Each agency carries out one or more of these responsibilities. Each one has unique information requirements associated with its responsibilities.

Regardless of what state you come from, whether in the North or the South, on the East or the West Coast, or somewhere between, the following probably sounds familiar: a growing demand for health care services and limited financial resources to pay for those services. State legislators and agency administrators are facing increasing pressure to make informed decisions about health care-that is, to make decisions based more on data and less on gut feelings or anecdotal stories.

As you might expect, the different uses of the information in the statewide hospital discharge database maintained by state data organizations are unlimited. They are certainly too numerous to cover here. But let me briefly review a list of the specific uses that have been made of aggregate hospital discharge data in North Carolina.

- Many studies of hospital utilization patterns to help analyze access issues, both for facilities and services.
- Several analyses of physician practice patterns.
- A few market studies.
- Data used for consideration of providers for selective contracting arrangements.
- Data have also been used for consideration of certificate of need requests to build new health care facilities or to provide new services.
- Data have been used to develop targeted community health education and prevention programs for selected public health conditions.

The ways in which health data-hospital discharge data specifically-have been used by state government agencies is perhaps best illustrated by the specific questions being asked.

- The legislature has allocated $150,000 for educational programs on prenatal care as part of the state initiative to reduce infant mortality. Given the limited amount of funds, what counties should be particularly targeted to receive funds?
- As part of a larger cost containment initiative, the state Employees' Health Plan is considering submitting a proposal to the legislature requesting permission to selectively contract with hospitals for high-cost, high-tech procedures. What hospitals in the state do the 10 most expensive procedures? What is the average length of stay and average cost for these procedures across these hospitals?
- The state Division of Mental Health wants to ask the state legislature for funds to increase the availability of local outpatient mental health services through the county health departments. Which counties have the highest hospital inpatient utilization rate for mental diagnoses? What is the profile of this population by county of residence-age, sex, length of stay, charges? What outpatient services are currently available in the county? What is the average income and educational level of the population in the counties?

Responding to these types of questions is not an academic exercise. These are real issues with which agency administrators deal. And they are using health data-specifically hospital discharge data-to help address them.

In summary, state agencies use health data for many purposes including policymaking., program development and implementation strategy, and surveillance of selected conditions.

Protecting Patient Confidentiality

State data organizations are very much aware of their public responsibility to protect patient confidentiality. And several mechanisms are in place to do so. I think of these safeguards and mechanisms in terms of layers, with the patient identifying data at the core. For the North Carolina Medical Database Commission, the various layers of protection include

- Enabling legislation that authorizes the state data organization to exist;
- Administrative rules or regulations governing the organization's activities, including the use and release of health data records;
- Various electronic security aids associated with the physical storage of the database on the computer, for example, audit trails;
- Controlled access to the databases, e.g., password access, commission review of all data requests; and
- Suppression of small cell counts in published reports.

One other layer of protection is the hiring of staff sensitive to the ethical and moral dimensions of confidentiality. Systems alone are not sufficient confidentiality protection.

This type of layered protection is in place in most other state data organizations. In addition, some state data organizations, like California, have specific written penalties and sanctions associated with breaches of confidentiality

The enabling legislation and the relevant operating regulations for state data organizations help enforce the protection of patient confidentiality in a major way. The language in the enabling legislation clearly sets out the intention that the data collected and distributed are to be used for examining patterns and trends in health care cost, utilization, and quality. The legislature never intended that the data collected and maintained in these databases would be used to take any kind of action that might harm an individual personally.

Many are probably aware of the sunshine or public record acts on the books in states allowing public access to information maintained in government office files. The enabling legislation authorizing state data organizations usually contain a provision exempting the databases maintained by these agencies from the public record act.

The Medical Database Commission in North Carolina does not release patient-level data to anyone. However, state data organizations that provide patient-level data to researchers have implemented some additional safeguards. They include

- Signed agreements between the researcher and the state data organization. These agreements may include (1) written documentation of the specific purpose of study and data request, (2) restrictions on the specific uses of the data provided, and (3) destruction dates for the data files provided.
- Institutional review boards (IRBs).
- Limits on the products/outputs of the analyses.
- Encrypting and converting data elements with patient identifying potential (for example, encrypting the patient identifier and conversion of admission date to day/week/month of admission).

State Data Organization Challenges

The demand for health data to make more informed decisions for purchasing, planning, policy development, providing care, etc., is growing. Health data of all sorts-outcome, utilization, charges, costs-will become an integral part of whatever version of health care reform is fmally implemented, whether at the state or federal level.

State data organizations and other state agencies that collect and maintain very large health databases are getting more and more requests for health information. State data organizations are facing five major challenges, not listed in priority order.

The first challenge is the need for a unique patient identifier, even though only aggregate data are released. The value added to the types of research and policy analyses possible when a unique patient identifier is included in the database cannot be overstated. We must keep in mind the benefits of the research and the interest of the researchers. What is of interest to the researcher is the ability to identify a single unique patient--different from any other patient. His/her personal identity is irrelevant. The identifier necessary to single the patient out as unique may be something other than name or social security number. But whatever it is, the identifier must be used every time that patient interacts with the health care system.

The inclusion of a unique patient identifier in the database allows health services researchers to

- Conduct longitudinal studies;
- Link different databases resulting in a more enriched data file for analysis;
- Avoid duplicate counts of patients; and
- Construct patient episodes of care-that is, to study a patient's treatment course across different provider settings for a particular illness.

The second challenge is linking of data files. It will become increasingly necessary to link data files to analyze the utilization and cost experience of populations *across* provider settings. Linking health data files may involve other data files; for example, files with income and education data.

In some instances, the issue of linking places state data organizations in a dilemma. State data organizations maintain health care charge and utilization information that can significantly add to the analytical value of other data files. For example, take the linking of hospital discharge records and birth records to add inpatient charge, utilization, and third party payor data to the birth records. Birth records already have patient names and addresses on them. The value that such linkage can add to maternal and child health studies is indisputable. But have we violated patient confidentiality if the hospital discharge data file is being linked to a data file that has a patient name on it? Are we compromising patient confidentiality even if the state data organization does the matching?

The third challenge relates to increased access to health data files. The need for analysis_ and not just data tabulations-in state government is acute. Although state data organizations are very rich health data resources, the resources necessary for sound research and analyses often are inadequate. Yet the analyses possible could truly benefit policy development and administrative decisionmaking.

Unfortunately most state data organizations that collect health data do not have the analytical

resource capacity to perform the necessary analyses and research studies internally. Much of their time is spent keeping the data collection and management functions intact. State data organizations will be pressured more and more to analyze the data collected. One beneficial way to do so and to ensure reliable results is to enter into collaborative arrangements with researchers and policy analysts. This will require increased access to the collected patient-level data. State data organizations will have to develop reasonable data release policies, specific to researchers and policy analysts, that still ensure patient confidentiality.

Another development that is quickly coming on the scene is the creation of community health information networks. The October 19, 1992, issue of *Modern Healthcare* had a feature article on this concept. Once this concept gets off the ground, I predict even more pressure for state data organizations to participate in these community health information networks, thus resulting in increased access to health data.

The fourth challenge relates to the growing need for automated decision support systems for health data. Although state government is comprised of various agencies that function as health care payor, regulator, policymaker and provider, data are not always readily available or in a format that can easily facilitate decision-making.

In the private sector, business executives have eagerly embraced the technology to convert data into information for decisionmaking. Software companies have responded by investing their development resources in decision support systems for use in the private sector.

Let me assure you that the need for that type of support is equally urgent in state government. Health policy development, reimbursement schemes, selective contracting resource allocation-these are all very real issues for state agencies. The challenge is there for collaborative efforts between state agencies and organizations in this audience to deploy this technology throughout the government sector.

The fifth challenge, and one that encompasses all the others, relates to greater protection of electronic data files. We must minimize opportunities for unauthorized access to health data files. Obviously, these files must be protected from hackers. But they must also be protected from organizations that are challenging interpretation of state public record acts to allow access to electronic computer files maintained by state agencies.

State data organizations are tremendous health data resources. States have taken a number of steps to secure confidentiality of the data collected, while at the same time trying to meet the many demands for health data. ◆◆

Administrative Uses of Health Records: Monitoring, Government Systems, and Law Enforcement

Florence Rice
Founder
Harlem Consumer Education Council

Privacy is a myth in the minority communities as it relates to medical records, treatment, and diagnosis.

Now that we have third party payor systems paying medical bills directly-it does not matter if it is an insurance company or government pm-grams-they want to know what their money buys.

It does not matter if your doctors are strong protectors of the privacy of their patients. The third party payments and the wide-spread use of computer databanks in the insurance and health industries make confidentiality beyond the control of the practicing physician.

Because of the tradition of the Hippocratic oath in medicine, people are shocked to discover that medical confidentiality does not exist by law. Nor does any law prohibit a doctor from revealing private information about a patient without a patient's consent. The only sanction is in the ethics of the profession.

> *... and whatsoever I shall see or hear in the wurse of my profession, as well as outside my profession in my intercourse with men, ijit be what should not be published abroad, I will never divulge holding such things to be holy secret.*
>
> *-Hippocrates, Greek Physician*

This is part of the oath to which the Greek physician, regarded as Father Medicine, adhered. Doctors seek to uphold the standard of the oath. Hippocrates did not know about a third party payor doctor.

The most damaging invasions of privacy are caused by doctors, nurses, and other medical staff who simply gossip too much. You find that they are more than willing to talk to the press or anyone else about patients' conditions without first checking with the patients or their families.

The medical professions carelessly discuss patients conditions openly at affairs and when treating other patients. We often visit doctors who will discuss other patients with similar conditions. Although the second patient's condition is the same as the first, it is not the interest of the individual. The individual has a right to decide whether medical information, even routine information, should be disclosed in such a fashion.

Yet, these same medical professionals will tell that same individual why they, the patient, cannot share or know the same medical information about themselves.

The courts subpoena medical documentation, medical professionals testify in court, and medical colleagues write books about patients in the name of scientific research.

Automation in the medical system has been a long-term practice through various means without the patient's knowledge and consent. A system of denying the minority communities the right to privacy has been in place ever since the practice of the medical profession began.

Automation is defined as a manufacturing system in which many or all of the processes are automatically performed or controlled. Instead of being verbal or written, our medical history will be an electronic control device. Once again, our minority communities are unable to prevent this kind of exploitation, and their privacy is invaded.

We found that in our communities we have the most aggravating invasion of privacy. An example of this invasion of our privacy occurs when patients sign language authorizing "any licensed physician, medical practitioner, or other person" to disclose information. Once this is signed, this documentation becomes a permanent record and is used at any given time by any agent of any profession.

We find this practice frequently when we apply for insurance coverage of all kinds. Signing such statements automatically forces us to give up our privacy. Every time information is released or requested, the consumer is to be notified of the request and its source and asked if the person wishes the information to be released. This is not a practice within the minority community.

Once this document has been signed, anyone can photocopy this information and present it to any hospital, insurance company, or doctor to receive information on the individual. The insurer can predetermine the kind of treatment an individual will receive or if it will insure the individual or deny the individual his/her request.

Signing an authorization opens the avenue of medical information that continues to flow to the insurance company investigators, company, medical information bureau, and employers.

Some of our government bureaucrats feel that medical information is their personal property. For example, the secretary of Health and Welfare of California under the government of Ronald Reagan walked off with 1,500 reels of computer tape containing millions of California citizens' medical insurance programs (MEDICAL). He wanted to use them for academic research.

As I look to leave this world as an African-American, I shudder to think what effect health/police/school records in an institutionalized racist society will have on my great-great-great grandchildren, who will be labeled and categorized as they enter the 21st century. ◆◆

Administrative Uses of Health Records: Monitoring, Government Systems, and Law Enforcement-Discussion

Janis Curtis, M.S.P.H.
Assistant Vice President for Special Services
Duke University

Florence Rice
Founder
Harlem Consumer Education Council

■ **Participant:** I represent the Privacy Bights Clearinghouse in San Diego, California. We run a hotline for Californians interested in learning more about their privacy rights. In three months' time, we have received about 6,000 telephone calls. We are getting more and more calls on medical privacy questions as time goes on. A common theme for many of those calls is the harm that comes to patients when the health care provider-whether the doctor, the nurse, or the clerical staff-releases anecdotal information or gossips, as you said, or the staff in the photocopy room copies too many pages and lets loose inappropriate information, say, for an auto accident insurance investigation.

We have heard quite a few cases of very loosely guarded information being let loose. I think back to the World War II poster, "Loose lips sink big ships." I used to be a librarian and we had a very strong code of ethics about releasing personal information about the kinds of books that people take out, who was checking out books this week versus last, and what the topics were. But I have not heard a lot of talk about the importance of educating people who work at all levels of health care facilities. It seems like an awful lot of harm that comes to people comes from outside the restrictions of research studies; it is really anecdotal gossip information. We have seen cases going as far as somebody's medical information bureau (MIB) report, which haunted that person because he/she could not receive life insurance.

I wonder if either of you have any recommendations for improving the gossip or anecdotal information situation.

■ **Ms. Rice:** I would like to see this taught in school as a part of consumer education. I would like to see that people are taught their rights. I am doing something with 'senior citizens, but it is a slow process. I would like to see some of these facilities have more education and information. I am also disturbed that I have to wait until I turn 90 to learn about health, when that should be going on all the time. I recommend having people informed; that is not being done at the local level.

■ **Ms. Curtis:** I guess I would take it a step further. I think people should be informed, and I also think they should be held accountable. There should be an employment requirement. When I worked at the Medical Database Commission, we collected a lot of paper claims and had people actually doing data entry My small staff, contract employees, were required to sign confidentiality statements. Any breach of that was grounds for immediate dismissal.

We need to go beyond just education. We need to hold people accountable and raise their awareness that this is a serious issue and we do not take it lightly. Although we do put a lot of attention on confidentiality for research purposes, we are lax in other areas. We need to tighten those up, as well.

Participant: Ms. Curtis, I was very interested to hear about the North Carolina hospital discharge database and particularly interested in the list of data protection measures that you seem to have in place. Is this a research and statistical database used for planning purposes, as

opposed to an administrative database used to affect particular persons directly?

■ **Ms. Curtis: Yes,** that is correct. The intent of the Medical Database Commission was to produce different reports that compared hospital prices and utilization and to support the decisionmaking process about resource allocation. It was not to take action against any individual person; it was never intended for that purpose.

■ **Participant:** That seems to me one of the most important things to say initially about a database-that it is a research and statistical database. But in terms of future uses, were you implying in any way that you could contemplate pressures for administrative uses of the database or, again, was it all in the sort of research, planning, statistical character?

■ **Ms. Curtis:** More along the statistical basis. The pressures that we used to get right before I left the Medical Database Commission were really more from the press for access to patient-level data. They did not necessarily want patient identifying information, and our rules prohibited us from releasing that. But it was not administrative pressure to take action against an individual.

■ **Participant: I am** at the Trishman Center and this is a comment more for the record. Both of you referred to minimal requirements for people who use databases to enter patient information or extract patient information. Many of the speakers here today have said that. I think the luncheon speaker even questioned whether a database user could sell the database. That is a serious concern from a mental health perspective of which the general public in America is not aware. A large majority of the direct care providers-mental health technicians, child care workers, whatever you care to call them-do not subscribe to any one profession, nor are they held in bound by any one code of ethics.

My boss has a wonderful story that unfortunately is true. In Massachusetts, 1,000 hours of training and a six-month apprenticeship are required to be licensed to cut my hair. But to play with the inside of my head, all I need to do is prove I did not recently molest a child; I can then go and work directly in a mental health setting.

Not having a code of ethics binding the large majority of people dealing with individuals in mental health institutions begs a serious question. How do we hold these people accountable for confidentiality of information exchanged in an automated record?

■ **Participant: I** want to make a comment about the use of employment sanctions against a data entry clerk. A data entry clerk is often categorized as a member of the working poor. And if the National Enquirer offers $50,000 for medical information, that employee's lost job is not really going to be much of a sanction. Some kind of legal sanction is also needed.

■ **Ms. Curtis:** I would offer immediate dismissal as one of a series of sanctions. I was not offering that as the only one. This is like a paradigm shift-we can hold those people accountable, and they have to be aware that they cannot do whatever they want without having to be accountable. That was my only point. But whether it is immediate dismissal or something else, we need to have something in place to discourage that type of behavior. ◆◆

Consequences to the Individual: Data Collection, Information Use, and Electronic Health Systems

Janlori Goldman, J.D.
Director, Privacy and Technology Project
American Civil Liberties Union

I want to address a misperception about privacy, one that we have heard echoed over and over today Somehow, privacy is considered a Luddite concept, and those of us who are advocates or naysayers are standing in the way of progress. In addition, these important integrated automated systems will fail if we put privacy and security protections in place. I have heard this notion in many different arenas. Many who are trying to put systems into place think that privacy will get in the way.

My experience is quite different. I have found that you can use technology as a way to enhance privacy. It can be used to give people greater protection for information and systems and greater security for the information in those systems-both to those who are using the information and those who have information in the systems-and as a way of giving users greater confidence in the system. You now hear industry groups talking about how privacy has become a customer service, something good for the business and not just something being done because public relations departments have expanded.

The Right to be Let Alone

Part of this image springs from one of the more traditional definitions of privacy and the one that a number of people have talked about today: the right to be "let alone." At least in my experience, when I think of the right to be let alone, I think of people who wrap themselves in cloaks-as grinches. They want to hide in their houses; they do not want anyone to know anything about them; they want to keep the government off their backs; they just want to be left alone. While there is, of course, an important privacy component in that attitude and one of the constitutional principles of liberty, a more positive and corollary component to the definition of privacy is one that Alan Westin first articulated about 30 years ago-the right to control information about yourself.

While we embrace the right to be let alone—when we are looking for seclusion, when we are looking for intimacy, when we are trying to take risks and we are afraid of being found out-the more positive aspect is that we choose to step into the world and participate. We can not always be let alone. At times you choose-sometimes voluntarily, sometimes not so voluntarily-to participate in the world, to step forward, to take advantage of a variety of activities and transactions. You may seek credit; you may seek a student loan, a job, insurance, membership in a particular group or a club. But the price of participating in this society should not be a loss of privacy. Even when you are saying you do not want to be let alone, you still want to be able to participate and not lose all of your right to control the information about yourself that you give up as a necessary condition of participating in those transactions.

This particular aspect of privacy is rooted in the traditional constitutional principles of autonomy, liberty, individuality, and self-determination. When you look at what you get in return when you grant this kind of privacy protection, it is very compelling. We heard someone earlier talk about how much privacy costs. They threw out numbers like $5 billion, $10 billion, $15 billion. I do not know what those numbers mean. I do not know how you measure what it costs to protect privacy.

The Cost of Nonprotection

But I can tell you what it costs not to protect privacy. It is also hard to measure in monetary fig-

ures, but there is clearly a cost, clearly a loss. Without privacy protection, the people will be afraid to step forward, afraid to participate in activities if the information about themselves is not safeguarded. We are already seeing this happen. We are seeing it most in the medical records context. People are going to be reluctant to give their doctors complete information for a diagnosis. They do not want it on their insurance claim form, which may be made available to their employer.

People are going to be concerned about even the doctor keeping the information. They do not want it to come back to haunt them at some later date. Some people are paying for their own HIV test, even though they are legally entitled to get reimbursed, because they do not want an insurance company to know that they took the test or know the result. Some people are withholding information about family histories. Some people are withholding information on mental health. We heard this morning that there is a good chance that if your employer wants information, then they will get it. No legal restriction prevents access to this information.

In other settings, privacy protection has been put in place to encourage the development of certain technologies and to encourage the use of these technologies. The electronic communications area is a good example. A number of years ago, the broad consensus was that this country's wiretap laws were outdated, they did not cover nonverbal communications, and they did not cover the new forms of electronic communications such as cellular phones, electronic mail, and bulletin boards. The manufacturers of these devices wanted legal privacy protection; they wanted these new communication systems brought under the umbrella of the wiretap law so that people would buy them. They wanted to encourage people to use these devices. And so a broad coalition of industry groups, consumer groups, and the ACLU came together and worked with Congress to figure out how to update the law.

Video rental is another good example. Some of you may remember when Judge Bork was up for confirmation to the Supreme Court. Bork's video rental list was disclosed to an enterprising reporter who was trying to find out who he really was behind all his legal opinions. A reporter obtained access to Bork's video rental list, and we saw very quickly how all of Congress unanimously supported very strict legislation to prevent access to video rental lists.

However, what is interesting is that the industry has, in both of those and in a number of other instances, come forward to support privacy legislation because it is good for business. They do not want people to be afraid to rent videos for fear that somewhere down the line this information may be disclosed.

Expectations of Privacy

I would like to address two concepts that I have also heard discussed quite a bit today. One is the expectation of privacy. Industry will sometimes say, "Well, why don't we just figure out what the expectation of privacy is and protect that?" This is a real problem; most people's expectations of privacy have been so lowered and so eroded by the existence of new technology and current practices that the expectation of privacy they currently hold can barely be seen under a microscope.

If you go to court to have your expectation of privacy enforced, the courts will now tell you that most individuals' expectations of privacy are unreasonable. The courts use a reasonable expectation of privacy standard in determining constitutional protection. The courts have now found that where something is technologically possible, it is not reasonable to have an expectation of privacy So you look like an idiot if you expect that activities in your back yard might be protected from the prying eye of someone in a helicopter hovering 50 feet above. You might expect that anything you put in a locker when you are a high school student would be protected, or that once you put your garbage out on the street you should not expect that the police will come and rummage through it, looking for all kinds of things. If you expect that kind of privacy, you are considered unreasonable. So I would be very wary about relying on established expectations of privacy as the standard, especially when the industry is developing policies and practices that set our expectations of privacy.

It would be better if the Supreme Court decided that the constitutional expectation of privacy is very high, but that probably will not happen any time soon. We are looking to Congress to create legally enforceable expectations of privacy, expectations of privacy that people can look to and say, "I have this expectation. It is legally enforceable. The court is not going to say, 'How could you have expected that to be private?'" The protection should be in the law, which is enforceable and to which Congress has decided you are legally entitled.

The second issue is consent. You hear the sentiment, "Let people choose. We do not want to get in the way of people's freedom to choose." And what this is usually a code for is the "opt-out mechanism." One of the big problems with opt out-which I do think is a workable mechanism in a number of instances-is that it assumes an equal playing field, a level playing field. It assumes that when you are talking about consent, you are usually talking in some contract terms about equal bargaining power on the part of two parties.

But when you think about patients and doctors, or AFDC recipients and the government, or students and the Department of Education, you do not normally think of two people who are on a level playing field. The information, bargain is going to be a tough one, and one that will always be a disadvantage to the individual.

Florence Rice talked very eloquently about this very lopsided situation. In looking at information bargains and consent, one must talk about balancing. Mark Rotenberg has been very fond of saying lately that we can never balance privacy against some other competing interest, because privacy will always lose, particularly when one is talking about reducing waste, fraud, and abuse. Privacy is seen as the obstacle to the fulfillment of those goals.

A Separate Value

We must view privacy as a separate value, on its own, in individual terms. We must look at how all of this information will affect the individual. Privacy should be the paramount concern in looking at any system, in creating any system, in operating any system, and in any kind of practice involving personal information. The paramount concern should be protecting the information in the system.

Privacy must be built-in, as Willis said, at the front end. You cannot wait another five years down the road and say, "Now, how are we going to take care of this privacy problem? We have this list of horror stories, and Congress is holding hearings, and we are hearing about all these problems. How are we going to build privacy in?" Sometimes protecting privacy involves software design fixes. Sometimes it is a matter of building privacy in institutionally, so that people do not see it as an obstacle but as part of the routine practice.

Let me move into health care. As you have heard, in the near future we are looking at integrated and linked systems of information coming from providers, insurers, pharmacies, and employers. No comprehensive federal law regulates the area of health care data. Some states have laws, but they are not comprehensive, and they do not deal with the situation at hand. They will not deal with the information itself. Most state laws deal with who holds the record. Maybe the law regulates insurance, maybe it regulates providers of medical care, but it does not regulate the health care data itself. with large-scale integrated systems, we must focus on regulation of the information.

Again, as Willis said, professional ethics do not apply here. Even if you are looking a little bit below the law and saying "Well, maybe we have these voluntary self-regulated ethical restrictions," they do not apply to the thousands of people who are supporting these new infrastructures.

We have gone around and around on the voluntary self-regulation front. It does not cut it, and it is definitely not going to cut it in the area of health care. You may be able to say, "Well, voluntary self-regulation works for the good guys, for those in the industry who care about this issue and want to see the information protected." But there will always be the temptation for abuse. Voluntary self-regulation provides no enforceable remedy for the individual and no penalty. The company may have some internal penalty but that is not deterrent enough.

Last year we saw the big scandal with a number of people in the government who were selling information from the Social Security Administration, the National Crime Investigation Center, and the IRS for $25 or $50 a pop. With health care data, the temptation will be similar.

So we need to look at the breadth and sensitivity of the information involved and craft some kind of enforceable privacy and security rules to encourage the use of these systems. But they must include trust for the individuals and provide some kind of remedy for misuse.

Comprehensive Legislation

A couple of years ago, I said to some of my privacy buddies here in town, "You know, we really need some kind of comprehensive legislation for health care records." People rolled their eyes and said, "Oh, no, we have tried this already, and it did not work." People who were new just said, "There's not enough political momentum; this is never going to happen."

Well, the political environment has definitely changed. We now can have a little bit of faith that the health care issue will be number one. We need to use this opportunity to make confidentiality protection an integral component of any health care reform proposal that comes out of the White House and that eventually will go to Congress.

Yes, there is a lot of work to do. But everyone in this room has some role to play in this effort. The government agencies can come out with recommendations about how to protect information. We hope that Congress will hold hearings on this issue. Those hearings will probably be one horror story after another; otherwise, we will probably never see legislation. The National Academy of Sciences is coming out with a report on confidentiality and regional health data networks. One of the critical tasks for all of us is public education.

Most people understand on an incredibly visceral level that the release of information about their medical history is terrifying. They do not think they have much choice about going to the doctor or filing the insurance claim form. They are not sure that their employer can see the information there. But if you talk to people and you let them know what the risks are and what is at stake, most people will say, "This information must be protected, and I want some control over how it is used." In the same way that the credit records issue has really galvanized public opinion in the last couple of years, and a couple of years before that the caller ID debate, people will see this is something that affects their daily lives.

If at any point our momentum wanes, we must remember that one of our strongest privacy protection laws on the books today is the video rental list law-the Bork bill-and yet we have no comprehensive legislation on health care records. If things look really bleak, we may hope that some enterprising reporter gets access to and publishes Robert Bork's medical records. ◆◆

Consequences to the Individual: Data Collection, Information Use, and Electronic Health Systems

Madison Powers, J.D., D.Phil.
Senior Research Scholar
Kennedy Institute of Ethics
Georgetown University

Today, I am going to begin by talking about something no one else has spoken about-swimming pools, construction sites, and abandoned refrigerators. You might wonder what that has to do with data banks and health care information. It actually has a lot to do with health care information. I only realized that when an old law school classmate reminded me of a doctrine I had not thought of in many years.

In tort law, there is a doctrine known as *attractive nuisance.* In essence, it suggests that unlike the swimming pool operator, construction site manager, and disposer of a refrigerator, young children have vivid active imaginations regarding the potential uses for these objects. They see nothing inherent in any of those items that defines its potential uses and purposes. So these items become attractive nuisances because they provide children with new places to play. But the swimming pool, construction site, and abandoned refrigerator pose great dangers. When such things are known to pose great dangers, and those who find them attractive can imagine purposes that their owners do not intend, then those who operate or control these items must limit the kinds of predictable harm that may ensue.

Reevaluating Need to Know

If we are going to move toward the creation of large health database systems, we need to undertake a wholesale reevaluation of our standard conception of the need to know. Just as refrigerators and the like carry with them no essential purposes inscribed upon them, nothing is written in the heavens that tells us who has a need to know. It may well be that many of the claims made on behalf of a need for some to know personal, medical, or health information about others are nothing more than social artifacts of a particular set of dispensable social arrangements. Under one kind of health care financing system, for example, certain people will argue that those who pay the freight have a need to know. If that health care system provides insurance largely through employment, then the number and identities of those persons claiming a bona fide need to know increases greatly.

Questions regarding the need to know are always nested in an analysis of our larger social institutions. Hence, I think that analysis of our larger social institutions and the demands we have from various groups to protect privacy reflect deeper, more fundamental questions about distributive justice. These involve questions of allocation. And, different sorts of allocation questions are involved: the allocation of benefits and burdens; the allocation of risk and opportunity; and one thing I call an allocational question-the allocation of decisional authority.

Who will control access to information about us? Who will, by virtue of control of the access to information, control our destinies and control our opportunities to make life choices? If I am correct in my assumptions about how privacy questions really raise issues of social justice, then our current interests in rethinking the distribution of health care provide a natural opportunity to rethink health care privacy as well. Thus, my first suggestion is that we combine our reorganization of health data systems with a reevaluation of who has a bona fide need to know information contained in these data systems.

A Mixture of Good and Bad

Access to information has different value for different people. Some of the uses and some of the

purposes are good. But some of the uses and purposes are clearly harmful. Most, however, are a mixture of good and bad. If most reflect a mixture of good and bad uses and purposes, then we always have to ask: Who gets what? Who gets the good parts and who bears the burdens, accepts the risks, loses the opportunities?

What are some of the potential uses of medical and health information that directly raise questions of distributive justice?

- To gain competitive advantage (i.e., insurance companies, employers, and many others who can use health care for those purposes);
- To reduce costs;
- To get rid of costly employees and employees with costly families (one neurological deficit baby **can** ruin your whole week);
- To reduce costs in government programs that provide health services; and
- To decide how to rank available services when we cannot pay for all that we might otherwise want.

Other uses pose ethical problems other than one of distributive justice. In a variety of instances, gathering information is a valuable social currency in the workplace or the community, Willis Ware nicely labeled it as trophy value. Sometimes the ability to gain power over others, or the purely voyeuristic instinct that some of us have, may be what matters most in our need for privacy protection. These are things people rightly worry about in addition to loss of economic benefits or opportunities. Privacy is a buffer against that voyeuristic dark side, and its value has nothing to do with the struggle for economic advantage or the achievement of institutional aims, such as cost-containment or ranking health care priorities.

In short, innumerable harms are done to a variety of economic, social, psychological, and dignitarian interests for which privacy protection matters.

Other more noble goals and purposes are attached to increased access to medical information: advancing scientific knowledge; improving public health in general; improving individual patient care; making physicians and other providers better skilled and more up to date; and providing other caregivers with appropriate feedback and information.

The list can go on. But information is a source of power, a source of ability to make decisions for oneself and to limit the decisional opportunities of others. It is something fought for and prized. Every time you find, on the one hand, a debate between strong privacy advocates (what Alan **Westin** likes to call privacy fundamentalists) and a variety of others who oppose them, we find a struggle to decide who controls the essential terms of our social relationships.

No matter how much either side is motivated, either by noble or sometimes selfish and distasteful ambitions or by sometimes laudable purposes, it is never a simple matter to sort out the competing claims by reflecting on privacy rights alone. Underneath is always a power struggle between competing visions, both of them good, and of whose interests ought to predominate.

My second suggestion, accordingly, is that the privacy protections we need must be effective against the powerful, whose motivations may be well-meaning but not consistent with the best interests of others, even though no harmful consequences are intended.

Nonexistent Health Data

The focus upon the special importance of protecting privacy in relation to health data particularly exercises so many people for obvious reasons. One not-so-obvious reason is that no such thing as health data exists. The point is similar to the one about refrigerators--things do not come with their essential purposes inscribed upon them.

The very idea of health data is an entirely conventional notion, with no limit to what might fall within its definition. If, for example, we are good clinicians, we want to know a great number of things about people. We think it is important to being good pediatricians or good geriatricians that we know things about life style, psychological matters, or familial concerns.

We are incorrect if we think of the practice of medicine as narrowly focused on clinical or laboratory data. We must recognize that medical care practitioners, as well as epidemiologists and other researchers, have a more expansive view of health; and accordingly, they increasingly seek to know more, not less, personal information.

Some people have suggested limits to such demands because of the marginal utility or the marginal cost effectiveness for each new bit of information we obtain, particularly if that information is to be stored in retrievable computerized format. But as any good practitioner of

cost-benefit analysis or cost-effectiveness analysis will attest, we can think of the potential cost savings from newly imagined uses to strengthen the case for gathering more information. That means that we need to think more carefully about the kinds of information gathered from people now, about the ways it is used, and about the ways that people most fear it will be used in the future. Thus, my third suggestion is that deciding how much privacy protection is justified depends on what we permit to be included in health data systems.

Replacing with "Ought"

Let us think for a moment about some empirical questions: What does a patient know? What does a patient expect? What does a patient fear? And we can ask those same three questions by removing the "does" and replacing it with "ought": What ought a patient know? What ought a patient expect? What ought a patient fear?

Let me simply guess about some of what the patient knows, or better yet, some of what the patient does not know. The patient typically does not know what an epidemiologist, a health policy analyst, or a variety of other researchers would do with personal medical information. Typically, a patient has no idea what kind of information goes to them, or what the outcome of research is, or anything else of that sort.

Ought they to fear such research uses of information? My own guess is not so much. Over time, I have become more and more inclined to believe the representations of the research community and think that they have a very strong case for more and better information, and often with patient identifiers.

Certainly the practitioner needs information as well. We have difficultly thinking about eliminating him or her from the informational loop. However, everyone who comes into patient contact does not need automatic access to all that might be contained in comprehensive patient data files. I favor giving the patient more control over practitioner access than I am prepared to grant him or her with regard to researchers.

What about the third party **payor?** A place for insurance companies is not exactly written into the nature of the universe. And while I am not fully prepared to eliminate them immediately, my first, second, and third choice would be to do so as soon as practically feasible. All other options are negotiable after that.

What do people fear? Loss of employment, loss of insurability, loss **of** reputation, social standing. They also fear the loss of the ability to make their own way through life, to be autonomous, to be part author of their own lives, and to control their own destinies. Often one simply cannot make one's decisions without being able to keep various bits of information away from inspection by others. No clearer example could arise than in the abortion context. When people talk of decisional privacy as somehow connected to informational privacy, this is not a conceptual, but rather a functional link. Frequently, persons simply are unable to make autonomous decisions if they cannot control the flow of information about themselves. They need to control not only what information is disclosed to others but what information is generated.

My fourth suggestion is that, other things being equal, we should prefer more individualized control over health care information, when it is collected, and how it is used. The primary exception to this principle is when the potential for overall social benefit is greatest and the risk of individualized misuse is least. Generally, the exceptions will involve research purposes.

Changing the Context

What about concerns regarding reputation and social standing? ***One*** of the ways that we might change the balance of privacy considerations versus other legitimate and important social goals would be to change the context in which privacy considerations figure. Rather than balancing and weighing privacy against seemingly incompatible goals, such as research, we might consider a strategy designed to make privacy less important. **Rights** only matter in circumstances where real interests are seriously threatened. Remove the threats to those interests, and rights wither in their importance.

So one of the ironies about asserting rights, or the rights of privacy in particular, is that they are highly contingent in their importance. They, too, are not written in stone. We did not come into this world with some of these deep privacy rights. Some rights are probably like that, but many are purely a function of the way we find ourselves in society and of the distribution of power, authority and the like. If some especially serious concerns are identified by many as among the most salient, and those concerns have to do with employability and insurability, then it seems to be at least an important option to start with a reexamination of the way we structure

availability of health care and of the present connection between employment and insurance.

This leads to my fourth suggestion: sometimes what will be most important to achieve is not greater privacy protection but **more** fundamental institutional reform.

The question that Dr. Clinton asked this morning is whether we will help make the case that there is **great** value in some people knowing mom about us than ever before. One of my suggestions is that the way to make that case would be to agree that some of us ought to know even less about us than ever before, and that we ought to eliminate some of the adverse consequences of some of us knowing more. I am prepared to make that trade, particularly when I consider the utility of improved research, of an enhanced ability to judge what kinds of interventions and therapies are useful, and of an informed basis for making decisions about budgeting.

Nonetheless, even if we do away with some of the identifiable sources of threats to privacy concerning our health care finance system, we will still have concerns about what to pay for when everything cannot be paid for. So let me suggest some of the other privacy harms that we should continue to worry about even after health care reform.

Not all harms associated with loss of privacy flow from the loss of individual privacy, or from the identification of a particular individual, or from the linking of information to that individual. Some of the harms from the health data system are likely to be harms to classes of persons as a consequence of aggregating data without personal identifiers. What kinds of harm are these? The kinds that I imagine will be a result of information collected and used to set budget priorities. Some people will be losers; some people will be winners, depending on how cost-effectiveness analysis and various other economic analysis techniques are used for deciding who gets what treatments.

Losers will be identifiable as classes. They will be losers only by virtue of the fact that we now have aggregated information about the health status and health risks of classes of people, not because identifiable information about any particular person is improperly disbursed in the system. Hence, sticky issues of **group** privacy rights are likely to emerge in the not-so-distant future.

Classifying Sensitive Information

What about the practice of classifying information according to **sensitivity—e.g.,** drug use, alcoholism, HIV infection, or pregnancy histories? I do not want to abandon that idea entirely. However, what is most important is not society's determination of the classes of information, which in general ought to be kept under special lock and key, but what individuals will want released, for what purposes, and to whom. Moreover, my anti-essentialist philosophical thesis suggests that no essential definition of sensitive information, such as mental health or other forms, implicate **social** standing or stigmatize. Nor can we maintain forever a fiction that any particular type of information can be kept separated from all other medical and health data. For example, to the extent that we amass new genetic information, comprehensive in character, one of the consequences is that information (including false information) inevitably will enter into the care-giving arena, into the patient files, and into the mainstream of health information.

So if you want to argue that genetic information must be kept separate with special protections, you must acknowledge that not everyone using genetic information sits in a laboratory wearing a white coat, armed with a foolproof lock and key Information flow knows no boundaries, and a classification of relative sensitivity will not be an adequate way to protect it. My fifth suggestion is that any adequate system of privacy protection must improve the level of protection afforded to all health data or health records. It will not be enough to focus on the most worrisome cases.

Finally, we need to rethink privacy protection in light of the way that health information flows in a modem society. Health information.often is collected in one city or state, sent out to a laboratory in a neighboring political jurisdiction to be analyzed, and then sent to insurance companies and various other people in other states. So what is a person to suppose when he or she reveals information to health care providers? Even if the person knows all the laws, say, in Kentucky when submitting to a blood test, the person likely will not know where the information will go or how it will be protected when it gets to Nebraska. Information simply does not reside in or comply with state law.

There is, in my view, absolutely no excuse to continue the parochial system of state privacy regulation if we are going to think about a national system of health data. Thus, my sixth and perhaps most important suggestion is that a federal health care privacy law should preempt the outmoded and grossly deficient system of inconsistent state laws. ◆◆

Consequences to the Individual: Data Collection, Information Use, and Electronic Health Systems-Discussion

Janlori Goldman, J.D.
Director, Privacy and Technology Project
American Civil Liberties Union

Madison Powers, J.D., D.Phil.
Senior Research Sctiolar
Kennedy Institute of Ethics, Georgetown University

■ **Participant:** I am the program director of the John A. Hartford Foundation. For several years now, we have been trying to organize community-wide, statewide health management information systems and are supporting planning efforts in six states. Additionally, at least another dozen states have expressed serious interest in the concept. We find that when states, even those farthest along, get to the point of truly wanting to protect privacy and the confidentiality of data, they have nothing to work with and are crying for help. I cannot emphasize this enough.

If your ultimate goal is to protect the individual as well as an individual within a group and a class, and if everybody involved in these systems has that as a goal, the question I have is—well, let me just add to the scenario: If you get a call tomorrow from the White House that says, "We want to do the right thing, too," do you have right thing by way of federal legislation, ready in the drawer to meet the need?

■ **Ms. Goldman:** In the last couple of weeks in talking to people about putting together some legislative package to move as an integral part of any health care reform proposal to come out of the White House, people have asked, "What will it look like?" "What will it say?" "How will it work?" Part of that depends on what the proposal is.

But then, again, there is a way of drafting principles or rules that will apply to the information, regardless of whether we are looking at managed care or at one system. We do not have anything in the drawer, but we can have something in the drawer tomorrow. To craft some basic rules and create a basic structure should not be terribly complicated, if you are talking about protecting the information.

Where people have experienced complications is in dealing with the exceptions to the rules. The rules are not terribly difficult. When the FBI says it wants an exception to the law, and 'when researchers say, "Well, what about us?" and when other groups say, "How do you deal with our concern?"-then you really have to start fine tuning the rules and that is where we are going to see the long haul.

■ **Partlclpant:** I am not sure I am willing to accept that. I started off by saying-I am really taking your point-we start with the protection of the individual, and just put that right over here and say "No matter what comes down the line as far as design, we want something ...." We cannot anticipate what is going to happen tomorrow. So can you give me a handy dandy generic, all-purpose piece of legislation? I am pretty sure that any legislation developed will be in the generic art form, or a variation of the generic art form.

And I think the generic art form will say that the individual's identity will be sacrosanct under all circumstances, except when the individual actively permits access to the identification-the name of an individual. You do not need the name of the individual for anything other than insurance underwriting and the doctor's record. If the individual permits the doctor to use the record, that takes care of that use. If you decide that insurers can underwrite

to conduct community rating, then maybe you get rid of that problem, too.

So just start with a very simple world, protecting the individual.

■ Ms. **Goldman:** Let us make an agreement here. I will provide you with the simple start, without any of the exceptions or projections, but then I am not responsible for the pummeling that you will receive when you present this proposal. And maybe you will not receive any pummeling. But when I say this is something the ACLU would like to see as part of the reform proposal, there may be a different reaction. You might see that. But I would be very happy to provide you with the basic outline.

■ **Participant:** I think we should put on record here that 15 organizations are working on some piece of confidentiality measures. American Society for Testing and Materials has some great work, American Health Information Management Association, Computerized Patient Record Institute, you name them. I think we should put on record that it is priority to coordinate those 15 organizations as each organization comes up with some paper and then to merge all of those into one national strategy.

Now one could say that the American National Standards Institute Health Information Standards Planning Panel is trying to coordinate that. However, what really is needed, in addition to that, is something like this Task Force to quickly coordinate all those efforts and to have an organized method for coming up with a national strategy

■ **Participant:** I am from the Social Security Administration. This question may not really quite fit this forum, but since we have two lawyers here, I would like to take advantage of that.

The issue is at once very specific and very narrow. Throughout this session, we have talked about the importance of patient consent prior to releasing medical records. And in Social Security, we make many determinations of disability. In that process, we require medical evidence from treating physicians.

One of the problems in our processing of claims involving disability is the time delay in obtaining medical evidence from physicians' because of the patient consent. I have thought about possible ways to redesign the system, taking advantage of technology, to compensate for the delay.

One possible option is that instead of using the paper to get the patient consent, I will call you as the patient and ask you to state, "I, so and so, give you the permission to get consent from Dr. so and so." I will then digitize that message. Many institutions and many providers now have personal computers. And nowadays, clipping a voice message by digitizing it and attaching it to a medical record is a very, very inexpensive method.

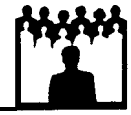
Thus, I can send the digitized voice record to you. You can play that voice in your PC and retain it as part of your medical record. Is that kind of alternative going to be acceptable from a legal standpoint?

■ **Mr. Powers:** Well, I can think of a technological fix that was once suggested. This fix is similar to going to the bank and opening an account. Someone closes their eyes, and we hit a key pad to get ourselves a PIN number, if we can remember it, so that we can go out and use our anytime teller cards. Presumably or reputedly, no one knows it.

We could do something like that from a physician's office or any other office, so that we have an available, accessible data bank. Someone could go in, key in, enter into their medical record, answer a series of questions-and essentially have computer initialized consent. I do not have any faults with the legal or ethical ramifications of that, but it seems to be perhaps a technological fix.

■ **Participant:** In our deliberations and discussions, we have most often focused on what I would now like to describe as the first order discussion of privacy: How do you control access to medical records? Who has a right to access medical records? How do we control the right to get access to medical records? Who has the right to decide these questions? And the usual analysis comes to the point of authorization. The individual has the right to control the access to his or her medical record or other kind of record.

The usual problem with that, as Ms. Goldman pointed out, is that too many of the situations were not on level playing grounds. It is disingenuous to say that I have the right to consent to access to my medical records, when if I do not consent, I do not get medical care. The doctor must have access to my medical records. The insurance company must have access to my medical records or it will not pay my insurance. I cannot very well say, "I would rather not have the insurance company find out about this, thank you."



So we have proceeded in some of our discussions to the second order of discussion. Let us put aside the question of who has access and how we control it. What can you do with the information, once you have it? Is the proper course of action for society not to focus on whether X institution can have access to some information about me, but to prohibit them from doing certain things based on that information? For instance, can we prohibit an employer from firing me because of particular information that it finds out about my medical situation, my family's medical situation, my genes, or whatever?

I think that Mr. Powers has really pushed us to the third level of analysis: How do we design existing social structures so that access to this kind of information becomes less sensitive because it is less useful? We do not have to prevent people from getting access to it. We do not even have to prohibit them from doing particular things with it, if we change the social structures so that they do not have any interest in doing those things with it, once they have it.

These are very difficult questions and the directions that you broached-and actually did more than broach-raise all sorts of difficulties. But our thinking about these questions is not complete, unless we take those kinds of approaches into account.

■ **Mr. Powers: Yes,** it is always good to look at these things in context. The problem with the specialization in the American system is we always look at things in a vacuum. But in Somalia, for instance, we do not need to send the troops in to stop famine if everyone has plenty of food. Many of the things we talk about in this health care context relate to the kind of health insurance system with huge numbers of people who do not even have health insurance. We have an increasing economic pressure to start singling out people that are more insurable and that requires more personal information. As long as it stays in place, that will be motivating to greater invasions of privacy and greater amassing of personal data. I really fear that genetic screening could turn into a search for the master race; the only people we really want to cover are the healthy ones.

But I also want to add a word about institutional memory. As mind boggling as it seems, a lot of work is being done on this issue. The Privacy Commission has laid out a very long and detailed chapter about medical records. The House Government Operations Committee has a 1980 committee report on medical records legislation. The EC has its own work, "Guidelines on Medical Records," and certain European countries have their own medical records statute. So there are many starting points; legislation is in the drawer. But as Ross Perot said during the debates, these plans are gathering dust and, obviously they need a lot of updating. But it is not like we have nothing to start from.

■ Participant: I believe that there is a 1985 model or act, too?

■ Participant: Yes, there are a lot of models, as we have pointed out. However, Ms. Goldman points to the problem of how these bills are structured. We have fought applying a statute to some particular institution or organization, saying, When you get information, you must handle it in a certain way."

What is being proposed now is that we apply the rules to the information wherever it goes. This presents a somewhat different drafting problem. Just to pull out the existing model will not be adequate. They all follow basically the same style-the Privacy Commission recommendations, the 1980 bill from the Administration and the Hill, and the model state law of the National Conference of Commissioners of Uniform State Laws. They all assume application to a particular type of institution and, indeed, they really only cover providers. We have been hearing here and we are aware of information about health that appears in all kinds of other places.

So it will take some pretty attentive drafting to write workable rules that follow the data around, wherever it goes. ◆◆

The Changing Health Care Environment

Deirdre Duzor, M.A.
Director, Division of Medicare, Part A
Health Care Finance Administration
Department of Health and Human Services

The changing health care environment is quite a broad topic and one that needs significant narrowing. So in addressing the role of information in the health care system of the future, I will consider it from two different aspects. The first aspect is health care reform-what is going on in health care reform and how information will play a critical role in the success of a revised U.S. health care system. And, secondly, I will talk about the possibilities that existing technologies give us to improve the health care of all Americans through gathering and using information.

This discussion of health care reform is based on the health 'care reform envisioned by the new Administration, to the best of our knowledge at the present time. Health care reform will be based on managed competition within global budgets. Each of those components has very important implications for information in health care.

One advisor to Candidate Clinton, who is probably advising President Clinton, recently said that managed competition will require an information revolution.

A dew Market Structure

Managed competition, just to lay the ground rules and give it a very brief generic definition, is a new market structure under which health insurance would be purchased by large numbers of people. This new health insurance market structure would be regulated or controlled by new entities called health care purchasing cooperatives (HCPCs). This new entity would go to competing health plans, be they HMOs or health insurers, to seek the best bid-that is, their lowest price-for a set standard benefit package.

This has tremendous implications for the information requirements and desires of both individual purchasers of health plans and these new HCPC entities.

The purchaser of health care could be either an employer or an individual. In either case, its choice of health plans will be made much easier in this envisioned managed competition system. A standard benefit package means that everybody would be pricing out the exact same product. No longer would confusion exist as to what is really covered under a health plan, what the copays and deductibles are, whether it is an individual deductible, at what point the family deductible kicks in, and what the catastrophic limits are. These issues would all be settled by establishing a standard benefit package.

Confusing Elements

One of the most confusing elements of choosing a health plan for individuals and small companies is understanding what they are getting for their money The model that comes closest to doing that right now is the Federal Employees Health Benefits Program. While I very much like the opportunity to choose my health plan from a long list of options, I find it very confusing to figure out what is really offered and whether it is a good value. This new system would eliminate these difficult choices.

The plans participating in the system would be offering the set benefit plan at a price negotiated or contracted with the HCPC. While it is unclear if the price would be set, and I suspect that it would not, the plan prices would have to fall into a rather narrow range for any company or HMO to be successful. Health insurance purchasers will not pay twice the price for an identical benefit package, and the price difference will be very clear to them, given the set benefit package.

So this system will virtually eliminate the two major confusing elements to figuring out how to purchase health care. The benefit package will be identical in all plans and a pricing structure will narrow the differences in cost.

Once the system is in place, the health care consumer will look to other elements to choose what to purchase. Consumers may begin with simple and obvious things like where the service is provided and who the providers are. They will then move on to the more difficult questions: How good is the care I will receive? An initial question may be easy: If I have a medical question, can I telephone and have a nurse answer my question?

Sophisticated Information Needed

But very quickly a'movement towards more sophisticated information about the health care provided by plans will develop. People will want to know more about what the care plans provide. As an example, consider diabetes management. If a member of your family has diabetes, you will want to know what treatment plan is used for diabetes. How successful is this method of treatment? For every aspect of health, people will demand to know more about what is provided, how it is provided, and the likely end result.

Likewise, the plans themselves will require a great deal of information. Remember, these will be competitive plans. They will have to stand up against the other plans in their area and compete for individual and group purchasers. To do that, a plan's priority will be maintaining a competitive price. The plans will need a great deal of information on how its providers are practicing. Plans will need to cut out any wasteful practices. If not, prices will rise and plans will be at a competitive disadvantage and eventually out of the market.

However at the same time, the customers are going to be questioning the health plan's quality of care. To deal with these requests, plans will be required to gather information to evaluate the health care provided to members.

The HCPC also needs information to negotiate with each of the health plans and to present plan options under managed competition to the public and employers in a set area. The HCPCs will be charged with a key information function and will need a great deal of information for managed competition to work. HCPCs must provide price information on health plans, information about the quality of care provided by each plan, and other informational demands of customers. As new measures of quality are developed, HCPCs will pass this information along to consumers to assist them in choosing what plan to purchase.

So all components-the purchaser, the plans, and the HCPCwill have a greatly increased need for information.

Developing Global Budgets

Let us turn to global budgets, the other element of the president's health reform plan. Global budgets should be information intensive. It looks easy to take the amount of health spending in a given time period, decide on an acceptable growth rate, and mathematically compute how much you want to spend in the next year. But that is obviously overly simplistic and too easy.

How can we be sure next year's target is not exceeded? How can we manage the health care sector to realistically hit that global budget? Success requires a rather sophisticated, very rich information base to monitor, in real time, the status of health care expenditures. We do not now have that level of data.

Much of our data on national health care expenditures is collected nationally It is based on participant sampling in the health care industry that is reliable only on a national level. We lack state-specific spending amounts. Using national data makes figuring out what button you push to turn off the spigot very hard. Is it valid in California or Michigan? We have a lot of aggregate data by type of provider, so we know with a fair degree of accuracy how much hospitals and doctors are spending. But that is hardly enough to tell us how to reduce expenditures to meet budget targets.

Some of the increases in spending may be unavoidable increases. An obvious example is spending on patients with AIDS. As the number of persons infected with HIV grows, the treatment costs will increase. And if the overall increase in health care spending is held at a fixed rate, then spending elsewhere must decrease. Someone needs to figure where "elsewhere" is on a real-time basis. It does little good if, at the end of November, we discover that we cannot make the target because the spending rate for the first nine months of the year exceeded our expectations. If that information becomes available in the final weeks of the year, the situation is too late to correct. So data needs to be gathered very quickly and analyzed very quickly with a high level of sophistication for global budgeting to work. Therefore, information needs will be quite intensive in health care reform.

Potential of Information Technology

Information technology now has a potential for tremendous advances in the knowledge and treatment of diseases and inpatient outcomes. Enormous amounts of information, and particularly, enormous amounts of health information on individual patients are available in this country But information is not centralized and it is on paper. Thick paper medical records are filed in vast rooms in big hospitals nationwide. Frequently, the data does not even get from the hospital to the physician who is providing outpatient care.

While we have an enormous amount of data, we do not have these data organized to allow maximum use. However, now we have the technology available to use the data-the computers are now big enough and fast enough. We have the technology that allows vast amounts of data to move from place to place. We lack the infrastructure, but we have the technology to support the needed infrastructure. For medical care and medical research, that means that we can direct the power of very large and very rich databases to answer questions about what works best in health care-what treatments and what protocols have the most effective outcomes for different population segments.

Take, for example, women's health. A lot of discussion recently has centered on disease processes in women. Our National Institutes of Health has begun a major initiative to conduct research on women because, traditionally, women have been largely excluded from clinical trials. Results of studies on men-for example, coronary heart disease treatment protocols—have simply been applied to women. Now, much concern is being expressed that women may react differently to types of treatment that are effective on men.

With a large data set, we can identify millions of successful treatment protocols and determine which categories of people benefit most from what treatments. Based on the analysis of our current data, we could very quickly turn the ship a bit and better target types of treatments provided for categories of individuals. But to do this, the data must be organized in a way to permit its analysis.

Expanding the gathering and use of health care information will and should happen. Obviously, this expected expansion has vast implications on privacy and confidentiality, the topics you have come here to talk about. This information has a tremendous power and a tremendous opportunity for some marvelous uses, but it also creates expanded opportunities for abuses. We must assess the policy questions involving privacy and determine the technological security system to apply to health care information to give the public a sense of confidence that their individual rights will not be abused. The benefits of this system, with the assurances of individual rights, are really something worth investing in, and that will benefit the health of Americans and, ultimately, everyone. ◆◆

Individual Rights and Expectations and Societal Needs

Larry Gostin, J.D.
American Society of Law and Medicine and Ethics and
Georgetown University Law Center Visiting Professor

Collection of information and privacy are charged issues. Information, they say, is power. Information can be used for the public good or the public health, or it can be used for purposes of less good or evil. To illustrate how charged an issue this is, the following three scenarios will demonstrate what the public thinks of privacy violations and information, what advocates think, and what medical professionals think, again in the public health realm.

The first picture is taken from a recent Larry King Live broadcast that discussed tuberculosis, AIDS, other infectious diseases. Prominent persons interviewed for the show made it absolutely clear that they wanted to get tough on persons with TB. They meant that they wanted to collect a great deal of information. They proposed mandatory screening for HIV and TB in all kinds of settings and mandatory reporting requirements of these diseases, including asymptomatic HIV or TB infection as well as partner notification for sexually transmitted diseases. To them, the government needs an aggressive and comprehensive program for collection and dissemination of information. That was the public's perception. They thought it very, very forcefully.

A second picture was at a Centers for Disease Control (CDC) meeting on HIV surveillance just a couple of weeks ago, where a clash occurred between the public health people and advocates. Many of the advocates were strongly against the idea of government collecting information. They did not want identifiers, and they did not want compulsory reporting requirements for HIV The advocates wanted anonymous testing and no reporting requirements.

The third picture illustrates what the medical profession thinks. The Axelrod case, decided by the highest court in New York State, was most interesting. The case pitted the public health community against the medical community Here was the medical community calling for much more aggressive uses of information, compulsory screening reporting partner notification programs. And the public health commissioner in New York was refusing to use coercion, saying that voluntary and confidential approaches were, by far, better. And so the case pitted, on the one side, the Commissioner for public Health in New York, supported by such organizations as the American Public Health Association, against the major medical societies in New York-the surgeons, the physicians and others, who were claiming more aggressive information collection.

From a public perspective, an advocacy perspective, and a medical and public health perspective, very little common ground exists about where we ought to go in resolving the balance between public health confidentiality and the use and dissemination of information. This presentation is intended to help you think through an assessment of confidentiality of public health information. How do you determine when confidentiality is more important than the collection of information? When is it more important to disclose than. to maintain confidentiality? I have been developing a human rights impact assessment for the World Health Organization in the public health realm. It will look at several factors.

- The purpose of information. Why do you need the information in the first place? This criterion examines the idea that information for its own sake is not necessarily a public good but must have a clear purpose.
- Will the collection of information achieve a compelling public health purpose? That is, by collecting the information, will you actually achieve what you hope to achieve?
- Will the data collection be effective as a health or public health policy? Will it present more burdens than benefits?

- Who will have access to the information? Will the information be disclosed either by force of law, authorized by law, conditionally through insurance, negligently? Who are the various groups that might have access to it?
- What are the impacts on human rights? Here, I am going to examine the impact on human rights from a stigma and discrimination point of view, from the individual's point of view, and also from the point of view of entire communities. This type of analysis is the product of one of the issues that I have been working on with the Council for International Organization of Medical Sciences (CIOMS). CIOMS is calling the idea macroethics, looking at the impact of confidentiality disclosures on whole communities, as opposed to individuals only.
- Are there any less restrictive alternatives? Can policymakers provide a system that will be just as effective with less invasion of privacy or confidentiality?
- How can policymakers resolve these conflicts? How do they balance the human rights impact with the need for information? How can they provide statutory and professional and other safeguards of privacy and confidentiality in order to enable them to collect as much information as necessary with as little risk to individuals and communities as possible?

The Purpose of the Information

Why do you need the information? Information is important; you will find this sentiment almost everywhere you go, particularly in the United States. Why would you not want to know the information? We see this all the time. We saw this after the Pan Am disaster. Even though the risk of a plane going down after a terrorist's threat was infinitesimal, there was a big call for the right to know. You also see patients claiming the right to know. Patients want to know a great deal of information about their doctors: How have they performed in previous bypass operations? Are they infected with HIV? Do they abuse drugs or alcohol? Doctors want to know everything they can about patients. Public health people, researchers, and epidemiologists all seek a great deal of information:

We first need to establish that information for its own sake is not good enough. We can justify asking those who want to collect information to explain what compelling public health purpose they have for that information.

If the government collects information—whether police, census, tax, health, public health, research-it should be able to justify the need for that information and if that information will be shared. This is the first criterion-establishing a clear, compelling public health purpose.

Compelling Purpose-Not Good Enough

The second criterion is that it is not good enough for individuals, government agencies, or others to simply state a compelling public health purpose. Stating a compelling health purpose is very easy: "I need the information for this individual's health" or "I need the information for the public's health." The entity requesting access must be able to demonstrate that access to information actually will achieve the public health purpose. And here, we must point out linkages between information collection and the service to be given at a later date.

We can look at the information collection in a variety of contexts. We collect information for health care reform or for managing health care costs. We collect it for epidemiology and research. We may collect it for reporting infectious diseases or reporting neglect and abuse of children. We collect information for health records.

The linkages between collection and the actual achievement of the good are complicated and need to be examined against the specific form of collection. Reporting infectious diseases is a prime example. I have just come from the CDC meeting where clinicians and policymakers have been trying to assess the balance between public health and privacy in HIV Many persons inside and outside the health care field feel strongly that we need to collect information of HIV seropositivity for various reasons. They take it as a generally accepted good that if the public health community knows where the epidemic is going and who is HIV infected it can provide services. The key issue is whether or not the information collection from the public health system actually achieves a public health good in the health care system, bearing in mind that often the linkages between these two systems are not very good.

No Guarantees

What might be the benefits of a reporting system or a mandatory screening system? One would be clinical. One could argue, for example, that if I had the information, then I would be able to offer early treatment and the services would be forthcoming. But persons with HIV infection know that if, in fact, the public health system collects information, it does not necessarily follow that services will be forthcoming.

How does that information reach the health care system so that patients actually receive those benefits of early treatment. Patients have no guarantee of adequate reimbursement for treatment. No extra resources are being put into services to make sure that person gets medical treatment. I can recall, for example, an earlier CDC meeting that was going to recommend routine hospital screening for HIV Every patient admitted into a hospital would be screened routinely for HIV At the meeting, a young, dedicated physician from Johns Hopkins was asked, " Wouldn't you want to know this information?" He repeatedly answered, "No, I do not want to know the information." After being pressed, he simply replied, "We are so overwhelmed in Baltimore with HIV infection that I cannot do any more. I am stretched to my limit." He was saying that having the information does not necessarily guarantee that appropriate services can be provided, so this linkage is very important.

Informed consent should be obtained from the person about whom the information is collected. The Council of International Organizations of Medical Sciences, together with the World Health Organization, is about to publish very important international ethical guidelines on human subject research. These guidelines rigorously investigate privacy and confidentiality. Significantly, the guidelines link consent to confidentiality and state that an informed consent for collection of information is mandatory for any person who agrees to become a human subject. And this need for informed consent is true not only for research but also for clinical care.

It seems to me that both law ethics and professional practice should link consent to confidentiality so that a person has control over information. The law requires this, inasmuch as the risks and benefits of treatment, research, or anything else that the patient is entering into includes breaches of privacy A person should know to what extent his or her privacy will be protected in order to make a fully informed decision.

A Personal Right

As a matter of ethics, the concepts of self-determination and autonomy mean that having control over personal information is a very important part of an individual's feeling of personal rights. And as a matter of professional practice, confidentiality is a very important part of the doctor/patient, public health/private citizen, and health care counselling relationship.

Another reason to give the information out is public health. For example, if an individual is HIV infected, has a sexually transmitted disease, or has a needle-borne infection that could be transmitted to a partner, many people argue that the information should be used to inform that partner about the risk. Clearly, that is very important. This is one of the cornerstones of the controversy surrounding confidentiality versus the right to know, illustrated in the Tarasoff case.

Information might also be needed for epidemiological purposes; for example, the information can be used to track epidemics. Here, you have to look at the information very carefully and decide whether you need the reported information. For example, some argue that self-reported information might provide skewed information, that you might be able to get better information through blind epidemiological screening. Any time you say the collection of information will achieve a public health purpose, you must be very, very clear and specific about how it will achieve that purpose.

Maintaining Trust

The third criterion considers whether the collection of data would be an effective public health policy. Sometimes, even when collection of information achieves good public ends, it has downsides. For example, if individuals know that when they come to clinics or other health care or public health settings for treatment the information collected may be disclosed to someone else, they may actually be discouraged from coming to that doctor or that public health clinic. Even if they do come, they might be discouraged from frankly discussing their problems with their health care professional. And so, one of the important parts of confidentiality is to maintain the trust between a health care professional or public health person and a patient, and encourage that person to come forward.

Pressure from the public and private sectors and the medical profession as a whole to perform more testing through routine screening might actually decrease rates of testing, because people would be driven underground, afraid of the implications of the results. The health care and the public health systems should take this seriously.

Accessing Information

The fourth criterion considers who has access to the information and whether the information will be confined to the health care or public health systems. For example, in the public health system, the CDC is one of the best government agencies for confidentiality. It is a rare case where the public health system has inappropriately disclosed information. However, we could think of many cases where the prison system, the police system, the tax system, or the health care system 'disclosed personal information. How do you tell a consumer or a patient, "This is a public health record and the public health departments hold this confidential?" People will not be able to separate various entities of government and make those nice distinctions about who will and who will not adequately pmtect personal information.

So one of the key questions is not only the protection of confidentiality, but the individual and public perception of how that confidentiality will be protected. Will the information go to employers, landlords, and insurers? Will the information go to family, friends, or community? How will it go there? Can it be forced by law? Will a court order or subpoena be valid? Can it be reported? Will there be mandatory reporting for child abuse, neglect, infectious diseases? Will it be authorized by law? If I had the time, I would review some current right-to-know statutes, with three pages of close, fine print covering exceptions to the principle of confidentiality that essentially overrule the actual rule.

Will information reporting be conditional? For example, as a patient you may have to give insurance companies information, not because you are required to-but if you do not, you will not get the insurance. So this is almost mandatory. Will there be a negligent disclosure-for example, an unintentional disclosure? All these things need to be considered.

Human Rights Impact

The fifth question is the human rights impact on individuals and communities. Here, it is extremely important to understand how the information will be collected and used. Will it be identifiable? Will it be nonidentifiable or purely anonymous? Will it be linkable information? Will a code enable you or someone to link it to another individual? Individuals are most afraid of linked or linkable information because it discloses sensitive health care information, it can result in stigma, and it can result in disclosure of a person's personal status or behavior. For example, it might disclose your sexual behavior or drug abuse behavior. It might disclose that you are a commercial sex worker or something else very intimate about you. Breaches of confidentiality may result in discrimination in jobs, housing insurance, or perceptions of fears.

Also risks affect communities, not just individuals. For example, collecting sexually transmitted disease (STD) information about a small school and pointing out that only a few people in that school have an STD might affect the entire school community. When you collect information by race, you might be implicating particular races or ethnic groups.

At the same time, you must ask if any less restrictive alternatives exist, if you could achieve the public health or health purpose in a less invasive way with less invasive of privacy, such as through blind epidemiological research, anonymous reporting, or using parallel systems.

To balance human rights and public health, we need to take confidentiality very seriously. Society should collect information only when it is needed.

Current state and federal confidentiality protections are a hodgepodge of inconsistent and incoherent protections. In some cases, like drug abuse and STDs, the protection is relatively high; for some specific diseases, like HIV, it can be high in some states and very low in others. We need a much clearer and consistent approach. We may need either a model state statute or a federal statute, something we are looking into very carefully **in our program. I hope that taking confidentiality and human rights seriously will be an important part of the future of public health.** ◆◆

Individual Rights and Expectations and Societal Needs

Michael Yesley, J.D.
Coordinator, **Program on Ethical, Social,and Legal Implications**
Los Alamos National Laboratory

As I listened to Larry Gostin's excellent presentation, I recalled my early bioethics experience in the area of protection of human research subjects. In the mid-'70s, our major concerns were the amount of risk posed to research subjects and the ability of some research subjects to give informed consent, specifically those who had a reduced capacity In those years, confidentiality was just part of a mantra. We would say "and appropriate steps are taken to maintain confidentiality," and move on to other topics. Now risk is no longer as much of a concern. The subjects have said, "Hey, we will worry about risk, do not protect us so much." But, on the other hand, confidentiality has become a much more significant issue. I will not say that risk has entirely disappeared, but a lot of refocusing has occurred.

Larry Gostin has given us an extremely useful. checklist of concerns about the use of medical information. I will talk about genetic information and genetic privacy as a case study. A number of questions Larry raised can be looked at in this context of genetic information. You will not necessarily find the answers right away, but you will be asking the right questions if you use his questions and apply them to the development and disclosure of genetic information about individuals.

Genetic information is a distinct subset of medical information. It is distinct because it represents a certain approach to medicine. It is also distinct because most people would consider genetic information to be especially sensitive, more sensitive than most other kinds of medical information, though not necessarily as sensitive as one area on which Mr. Gostin concentrated—HIV. But, certainly, genetics covers areas that are far more sensitive than medical information.

Asymptomatic Information

And why is that? Well, one reason is that genetics can provide information about an individual who is asymptomatic. It can diagnose a condition that will affect that individual at some point in the future, either with utmost certainty or with some probability Some genetic disorders are late onset disorders, such as Huntington's disease. Increasingly in the future, we will have an ability to detect a genetic susceptibility which, combined with an environmental insult, could result in a disorder. And so genetics is going to tell us intimate details about individuals who are totally unaffected at the time of the genetic testing.

Another aspect of genetics is that it affects other individuals-blood relatives of the individual tested, unborn progeny, and living progeny. Genetic information is also unchanging from conception to death. Science fiction writers and some physicians talk about making changes in us genetically, but that is a thing of the future. By and large, we must consider genetic information to be immutable. Genetic information shares with other types of medical information the ability to stigmatize individuals, both in their own eyes and in the eyes of other individuals.

The types of information derived from genetics are especially sensitive. Looking at this over time, we can assume that in the next few years we will be able to generate more and more kinds of genetic information. The sensitivity, in a way, will be compounded by the volume of this information. Genetic issues will grow in the future.

One reason people are concerned about the disclosure of genetic information is that the ability to identify a genetic condition precedes by many years, and will continue to precede by many years, the ability to do something about that disorder. The information is useful, perhaps, for reproductive planning, and it is useful for those who want to prepare for the future. But being able to diagnose a genetic condition does not confer the ability to do anything about it. And

so, a lot of questions are asked about whether certain information should be developed in the first place, since it will not impact any practical decisionmaking. In other words, we must ask a threshold question before we get to the question regarding to whom information about genetic conditions should be disclosed: Is it appropriate to develop that information about an individual? Under what circumstances is it appropriate to develop that information?

Genetic Privacy Studied

The March of Dimes conducted a study of public opinion about genetic privacy late last year. Approximately 60 percent of the survey respondents believe that someone else should know if one is a carrier of or affected by a 'genetic disorder. The great majority believe that a spouse or fiancee should be advised, 58 percent thought that an insurer had a right to that knowledge, and a third thought that an employer had a right to that knowledge.

At the same time, respondents indicated they did not know very much about genetic information or genetics. So, for what it is worth, the study collects intuitive responses, not necessarily knowledgeable ones.

The Human Genome Project is a $3-billion project to be conducted over the next 10 years, for a total of about 15 years, by the Department of Energy and Department of Health and Human Services, to map the entire human genome. The purpose of this mapping is not to discover the genes linked to different conditions, but the map's existence will greatly facilitate that discovery process. In the next few years, we expect many more genes to be identified.

Social and Ethical Issues

At the same time that the government is funding the molecular biology effort, Congress has recognized that the resulting increase in information will raise social and ethical issues. And so a certain percentage--3 percent for the Department of Energy and 5 percent for NIH, which add up to $7 million a year-has been allocated both to education and research efforts. The social-impact research will define social issues that arise as a result of the increase in genetic knowledge and make recommendations about ways to resolve them.

The Department of Energy and NIH have established a joint working group to oversee this social research. It has made recommendations for public policy in the area of employment and will make recommendations regarding health insurance. We have mentioned particular areas of genetic privacy in different contexts over the past day and a half, but I will now look at them in the specific context of genetic information.

First-employment, the employer's potential access to genetic information about prospective employees or current employees: Is that going on? Are employers doing very much genetic testing? At present, they are not. A couple of Office of Technology Assessment (OTA) studies, one several years ago and one conducted just two years ago, were based in large part on surveys. These surveys found that employers are not using genetic information to any great extent for the very simple reason that it is not cost beneficial. But as information becomes more available and easier and less expensive to obtain in unregulated circumstances, we can expect employers to use genetic information to a much greater degree.

Occupational Exposure

We can divide the testing that employers might conduct into two broad categories. One is occupationally related. Employers might be interested in learning if their employees or prospective employees are susceptible to conditions resulting from certain exposures likely to be encountered in the workplace. And before you immediately say, "Well, that sounds reasonable, why not do that," think about the other side of the coin. It may make more sense to clean up the workplace than prohibit a certain segment of society from working there.

Another type of testing that employers might conduct is not occupationally related. It is intended as an adjunct to learning the health status of employees and, particularly, learning which employees might incur greater health costs and become a greater drain on the self-insuring employer's finances. The Americans With Disabilities Act, **which we look to** these days when talking about employment discrimination, is somewhat ambiguous about its coverage relating to genetic conditions. Clearly, an expressed genetic condition would be considered a disability and an otherwise qualified worker would be protected from discrimination. But suppose a prospective employee had a late onset condition that was not yet apparent. Or suppose the employee was merely a carrier of a condition that could be passed on to children and that might result in increased health care

costs for the children. Americans With Disabilities Act may not protect the prospective employee from being told, "Sorry, we are not going to employ you because we want to avoid the costs of your future health care."

Recently, insurance coverage has received a great deal of attention. The situation with genetics is similar to other preexisting conditions. Many have said that the genetics provides another reason for universal health coverage to get away from individual underwriting because it provides another way to discriminate against individuals.

Unconsented Disclosure

Another area of concern about the privacy of genetic information is unconsented disclosure to relatives. Relatives may be very interested in learning about conditions that could affect them. But for reasons best known to themselves, individuals being tested may not be willing to disclose test results to their relatives. Reference was made to the Tarasoff decision, the duty to warn others about a substantial danger to them. The question **here is whether genetic information** rises to the level of being substantially important information that should be disclosed to relatives against the wishes of the individual patient.

A major area of concern is unconsented disclosure to the government. Should the **government** do more testing at birth or at marriage? As genetic testing becomes easier to **accomplish—** for example, in the future, it will be possible to isolate fetal cells in maternal blood, so genetic testing of a fetus will.become a noninvasive procedure-and as the government may undertake certain financial responsibilities, how much more information will the government want to know about individuals, either in the guise of helping private citizens or in the guise of saving money?

Data banks present a major concern regarding genetic information. Basically, two kinds of data banks exist-one has the encoded data from genetic testing; the other has the biological samples themselves, which are capable of being subjected to further testing. There are many different kinds of data banks, including forensic data banks maintained by the states, commercial data banks, and research data banks.

Identifying the Unknown Soldier

The military has a genetic data bank now. The military's data bank was set up with the good intention of ensuring that never again will a soldier be an "unknown soldier," never again will remains of American fighting personnel be unidentified. However, as soon as the Department of Defense announced that it would have genetic samples of all service people going abroad, it received a phone call from the National Cancer Institute. It recognized the potential research the database would allow and requested access to the information to perform various longitudinal studies. I join the other speakers who have referred to Alan **Westin's** writing and a question he raised about forensic databases-will the adoption or the initiation of these databases for valued purposes put us on a slippery slope to using the information for additional purposes that may not be so justified?

Sometimes information, in the absence of the ability to do something about what the information reveals, is not so useful. We should be particularly concerned about forcing the development of such information. We do not want to force information on people who do not want to know about themselves. The other side of that coin, however, is that when their actions affect others, they may have an obligation to learn such information.

Finally, I would like to mention informed consent. My experience with informed consent is that it is clearly not a panacea. Informed consent is often not informed, and it is often not voluntary It is given-or taken, more precisely-in the context of, "If you want this service or this opportunity, you will give us this information." Under those circumstances, the notion that the consent is voluntary is subject to great question. ◆◆

Individual Rights and Expectations and Societal Needs-Discussion

Larry Gostin, J.D.
American Society of Law and Medicine and Ethics and
Georgetown University Law Center Visiting Professor

Michael Yesley, J.D.
Coordinator, Program on Ethical, Social, and Legal Implications
Los Alamos National Laboratory

■ **Participant:** Mr. Gostin, yesterday, the group seemed to feel that, with legislation mandating confidentiality and privacy, we as individuals and our personal information would be safe. You discussed the need to balance human rights with the public health system's need or desire to access information. And you also mentioned state and federal legislation would be needed to insure confidentiality and privacy. I believe you made a reference to the confidentiality of patient records at drug and alcohol treatment centers and facilities.

So when I read the federal legislation on drug and alcohol treatment centers and the confidentiality of patient records, I noted the comprehensive and significant legislation that affords privacy, nondisclosure, and confidentiality within that piece of federal legislation. But when you read the court cases that base their analyses on that legislation, the courts appeared to be arguing entirely around any confidentiality or nondisclosure provisions and arguing out protection for the individuals. So despite the fact that we have state or federal legislation that protects the individual, the courts might not recognize it.

■ **Mr. Gostin:** As a general rule, the state of confidentiality law is enormously haphazard. We have an antidiscrimination law now that provides a model, even if an imperfect model, about what we can do with discrimination. It is not disease specific; it is very broad, ranging across different public and private sectors. Michael Yesley talked about the Americans With Disabilities Act (ADA). The ADA is imperfect because it does not speak to future disabilities, an issue that is very important for genetic information. So we are not sure exactly where it goes.

Insurance can be very weak. Although in the particular Supreme Court case that Mr. Yesley talked about, the McGann case, the court might possibly deal with it differently under the ADA. In fact, the Solicitor General for the Department of Health and Human Services asked the Supreme Court not to decide it, saying that these are cases that are better decided under the ADA. But I agree with Mr. Yesley that the situation is still very imperfect with a lot of problems.

But at least we have something. In confidentiality, we have nothing. We basically have a hodgepodge of laws on HIV, we have very incoherent distinctions at the state level between communicable and sexually transmitted diseases. We have specific federal protection of drug abuse, but not other areas. We have widespread specific research protection. I think we need a much more comprehensive, clearly consistent state and federal approach.

■ **Participant:** Mr. Yesley you said that people are less concerned now about risk and more about confidentiality. Originally, potential subjects or patients had a great deal of trust in physicians. But as they became aware of risks, we ultimately developed a number of protections, such as institutional review boards (IRBs), the Office of Protection from Research Risks, and the whole series of meetings and things like the President's Commission.

I think the same thing has happened with confidentiality. People had a high degree of trust in health professionals, but that has decreased. People are becoming aware of the failure of confidentiality provisions now that a wider group of people know the facts and/or have access. I wonder if you would comment on that relationship.

■ **Mr. Yesley:** I am not sure I understand the question.

■ **Partlclpant: The** consumer has shifted the trust in people involved in providing health care. They do not trust the confidentiality. Is the question not that they cam less about risk now that they know about protections against risk, but what protections are there about confidentiality? Is that responsible for their concern?

■ **Mr. Yesley:** I do not think that the concerns with confidentiality are arising from the subjects themselves, but rather from policymakers who are rightly concerned about the exposure. In fact, there is virtually no litigation on breach of confidentiality. There are not a lot of horror stories about breaches of confidentiality. I believe it is a real threat, but not one that has actually occurred.

■ **Participant:** We **are** currently doing some work in the area of confidentiality, particularly in matching ***or*** linking records. We have discovered a number of things about the concept of confidentiality. One is that confidentiality is often interpreted very differently by the person that signed the consent than by the person who wrote it. When we were looking at what happens when you design a scenario saying, "I would like your permission to link or to match your records," people have very strange notions about what these terms mean. Linking and matching are different to them. Sharing means a very different thing. And unless we can get some clarity, we will never have a truly informed decision on the part of the respondent.

We also found that people do not necessarily object to participating in a study one time. The problem comes when you start linking these databases. Ethically, you would have to tell the person and explain up front about the studies that could be conducted with these data, where the data go, and their purpose. Practically that may be impossible; yet you cannot avoid thinking about it.

A major concern pertains to the length of time a record can be kept. For example, in psychology, when you diagnose a mental illness, you keep the record for a certain length of time. After that, the diagnosis in certain circumstances is no longer valid; you must rediagnose. For the patient's protection, the diagnosis is not forwarded in the records later on in life. I wonder how we will deal with that when we start developing all these databases.

■ **Mr. Yesley:** In my experience, the design of informed consent statements is generally prepared for the researcher's protection. While intended for the protection of the subject, the researchers wants to pile as much information in as possible, often past the point of comprehensibility That is what researchers have told me when I have sat on institutional review boards. They want to make sure that the institution cannot be sued. If all this is out there, and the subject signs it, then that protects us. So that may explain why informed consent is not well understood. Protection of the subject is not the main goal of consents, at least in the eyes of those who often draft them.

As for additional or future uses of genetic information, most commentators would say that an informed consent should be specific and should cover the intended uses. If you want to make additional use of the information in studies not yet contemplated, then you should go back for an additional release from the human subjects.

■ **Partlclpant:** Most of us are just thinking about systemic general data protection legislation to insure medical confidentiality. Is there any need for more specialized legislation for HIV, sexually transmitted diseases, or genetic information? Or would tightly written federal or state legislation covering medical information confidentiality encapture the kinds of problems you have described and anticipate in the even more sensitive kinds of personal information?

■ **Mr. Gostln:** In questions of human rights, either in the discrimination area or in confidentiality and privacy, it is better to form common principles than to be disease or subject specific. When you do that, you have all kinds of questions to figure out; for example, what makes STDs different from AIDS? What makes AIDS different from drug abuse? What makes that different from genetic information? What makes that different from information about diabetes or something similar? With separate legislation for each of these, you would have difficulty justifying **why you have protected one over another.**

The real reason we protect ***one*** rather than another is a political justification-not an ethical, moral, or public policy one. I would love to see us at least make the attempt to find a more common ground and to find statutes that span large areas. We may not get something that is monolithic, but I surely think we could get something, for example, that deals with communicable and sexually transmitted diseases and then. with medical records in a more common and understandable framework.

That should be our goal. If we are looking at ethical, legal, and public policy research in this area, we should focus on those aspects.

■ **Mr. Yesley:** I would agree with that for most of genetic information. The one area where some special protection may be needed is for relatives of test subjects. But, generally, I would like to see the development of broad principles that would cover genetic and other sorts of medical information.

■ **Participant:** Mr. Gostin, I am concerned about the absence of legislation enforcement. Whether or not it is written tightly is somewhat irrelevant because legislation under the Americans With Disabilities Act and HIV confidentiality legislation has not been enforced well enough yet to support children who are wards of the state.

As an example, consider the case of Patient X, a 14-year-old female, currently in prison. She is HIV positive, a runaway, a drug user, pregnant, has a child who is positive and already in care, and has used up the end-of-the-line services in that state. No one will take her. I constantly get phone calls: "Can you, as a national resource center, please help with that? Help me find a place to put her." And when I call my good friends in any one of these states and ask, "Can you please take this child?" the response often is, "I thought you were my friend," and they hang-up. Legally, they are supposed to take her, unless they can prove that they cannot provide the "reasonable accommodations to meet her needs." The argument often is what you were stating, the lack of services on the other end, the lack of financial support in the agency to accommodate this young woman and others about whom I get phone calls.

And I am wondering what kinds of legal support can be put in place on behalf of children and teenagers who do not have a voice, who do not know their rights, and who are not adequately protected by current laws.

■ **Mr. Gostln:** Well, it is a broad question. You start with the idea that confidentiality protection through legislation is only a very small part of the answer, not the answer itself, and you gave a lot of reasons for that. Laws are difficult ways to protect human rights; they are difficult ways to look at ethical obligations. So when you use a law, you try to just frame it as clearly as you can, give it some enforcement capability.

I keep referring to the civil rights laws, ending with the Americans With Disabilities Act, because they give us a very thoughtful, long-lasting model that has considered carefully questions of clarity, of broadness of principle, of enforcement. And in each of those areas, I could talk about how the disability law or civil rights law address the question. It is not perfect, but it is a lot clearer and more thought out than work we have done in confidentiality. It is incredible that we are having this conference now on a subject of such importance with so little thinking about legislative protections and ethical principles in uniform ways across diseases and problems and age groups. ◆◆

Approaches to Privacy Protection: Policies and Guidelines

John Fanning, LL.B.
Senior Policy Advisor
Office of Policy and Evaluation
Department of Health and Human Services

We have heard a great deal about the need for privacy and the need for data, and why both are important. We are now faced with taking practical political steps to' do something about these issues. I believe that protecting information about people requires three things. It requires legal controls. It requires educated, committed professionals. Finally, it requires an aware, sensitive public. While I will focus on the legal control, this is by no means meant to slight the other factors.

No Comprehensive System

Some legal controls do exist, but there is no comprehensive system. It is interesting to note the words that people use: "hodgepodge," "medley," "pastiche," and so on. Basically, the law of health records is state law. A federal law, as we heard earlier, covers the vast bulk of substance abuse treatment data. But, by and large, health records are covered by state law, and it is very much a mixture. Some states have comprehensive statutes; others have an assortment of protections in the statute. Other states have a series of cases, making a common law set of principles about how data should be handled. Some of the states, which do not have comprehensive laws for health care providers, have laws governing little bits of health care such as particular types of institutions (state agencies, health data organizations), or particular classes of data, like mental health data. Even states with comprehensive schemes typically leave untouched health data that has migrated, shall we say, to other settings out of the providers' hands. The American public does not have a clear, comprehensive set of protections that it can easily understand.

In the late 1970s, attempts were made to pass a national law on this subject pursuant to the recommendations of the Privacy Protection Study Commission. An administration bill ultimately failed in a floor vote in the House of Representatives. Some people felt it was too regulatory some people said it provided too much disclosure, and others said it provided to little disclosure, and so on.

Privacy by Exclusion

To date, the heart of the process in writing a privacy law has actually been determining what disclosures should be allowed without patient consent. By and large, such laws have been designed to apply to particular entities or institutions, not types of data. There are some exceptions, but they are limited. Mostly, these proposals have been to cover health care providers. And what they typically say is that no information held by this class of entity shall be disclosed under any circumstances, except as provided in "subsection b." Then subsection b has a very long list of allowable disclosures that represent the policy choices by the people drafting the bill or working up the model law.

After the failure of that federal effort, efforts were refocused on the state level. In 1985, the National Conference of Commissioners on Uniform State Laws developed and published a model health care information act that followed approximately the same model. At about the same time, the first cases of AIDS were diagnosed and made public, emphasizing the need for a comprehensive sets of protections for health records. Instead, a series of very targeted, very narrow statutes dealing strictly with AIDS information was created. Often, now, with further scientific and medical developments, they do not work quite as well as when they were applied to highly specialized testing situations.

Dramatic Developments

So we are faced with deciding what to do now. We have had dramatic new developments that are pushing us along. We have had a proposal for a nationwide system of computerized patient records in a standardized format, accessible over sophisticated, brilliant telecommunications networks. We have also had proposals for a national health care program. It is now difficult to avoid thinking about the issue in a comprehensive way Everyone on the scene, including the major policymakers, recognizes that protection of the data is a major issue, if for no other reason than that the public will finally be alarmed at the prospect of centralized databases and will want assurance that these databases will be used properly. So new and better techniques for protection are needed at a national level.

It is difficult. The data appears in many places. Traditional law governing data was written to cover a class of data holder. But, now, health information appears in many diverse places. If you go to a physician and charge the bill to your VISA card, VISA will know the name of the provider and his or her specialty. Should this be considered medical information? Individuals may not want others to know that they saw a particular type of specialist. Do we cover the records in the hands of organizations like VISA? This type of issue must be thought out.

In addition, we have new ways of passing around information, and I hope Alan Westin will address this to some extent. The thinking that went into designing past statutes and bills was largely built around the paper record. Those working on these issues in the 1970s said the work was begun because of computers. With entirely new methods of transmitting information and the related hazards, we may need new protection techniques.

We must also reconsider allowable disclosures of information. What seemed appropriate in the late 1970s may not be appropriate now, when information can be transmitted electronically in a much more convenient fashion. I am not making any specific suggestion or recommendations along those lines. I am merely indicating one of the issues that will have to be rethought in light of the new and developing possibilities.

We have a large task ahead. A great deal has been done. The recommendations to the Privacy Commission and the earlier HEW report are very valuable. But, we have a great deal more to do now in applying those principles to a much changed situation. ◆◆

Approaches to Privacy Protection: Policies and Guidelines

Alan **Westin,** LL.B., Ph.D.
Professor of Public Law and Government
Columbia University

I feel myself tugged among three roles as I speak to you. First, I view myself as a privacy advocate who believes that the balance that society strikes among the competing values of privacy, disclosure, and surveillance requires continuous and passionate advocacy of the privacy claim, simply because such strong power and interest are behind the claims of surveillance and disclosure.

A second role is that of a social scientist who believes in a coherent and useful way to study the impact of technologies on society and thereby to understand the values of privacy and of privacy-protecting balances in a free society. Too often in privacy debates, we lack solid empirical evidence as to how technology is really unfolding in the world of organizations and how individuals' benefits, rights, and opportunities are affected by the interaction of computerization with the gate-keeping functions of complex society A social scientist must go beyond the easy journalistic speculations about how fast technology is unfolding to trace the impacts on individuals and affected social groups by organizational adoptions of technology

Third, over the past 30 years I have served as a consultant to a number of private and public organizations interested in confronting these issues in a proactive and responsive way They are seeking help in understanding the issue and in explaining internally to top executives why this issue must be faced, why new policies are worth the organization's time and energy and how this could earn them operational and organizational advantages in society.

Deja Vu

I want to discuss privacy and health records today from each of these perspectives. Twenty years ago I conducted a study for the National Bureau of Standards (NBS) and the Association for Computing Machinery on computers, health records, and citizens' rights. This creates a powerful feeling of deja vu, because *everything* I have heard at this conference was discussed in that report. There is absolutely not a thought, a problem, a dilemma, or a search for solutions that was not fully captured in that report. I note that, not because I wrote the report, but because I assembled the right group of advisors, researchers, and people on the firing lines; because we looked at all these issues; and because our recommendations-updated for 1993's environment--seem to me entirely germane.

Early in the report, I said that the driving force that may help us move forward in setting good privacy'policies was the probability that a national health insurance program might be adopted in the 1970s. That was the political launch pad that might have served as the catalyst for accomplishing something fundamental in privacy protection for health records. Now the possibility for national health insurance arrives as a new enabling image to dance before us in the 1990s. I hope it will do better for us in the '90s than it did in the '70s. Let us think a little bit about what it would take and how that might work.

In the executive summary of the NBS report, handed out today you will see the way I analyzed these issues in the '70s. I began with a description of the movement of individual identified health information from Zone 1: direct health care, into Zone 2: payment and quality care assurance, and then into a larger third zone, Zone 3: social uses of personal identified health information. This is the world of wider and wider circulation of identified medical information about individuals that is driving public concern and demanding a redefinition of medical privacy, confidentiality, consent, access, and disclosure policies.

For the study six real organizations were looked at as in-depth case studies of the way this

process was working and the real problems arising The types of organizations we looked at were varied-the Los Angeles Medical Center, the Martin Luther King Health Center in the Bronx, the U.S. Indian Health Service, Kaiser Permanente, Mutual of Omaha, and Multi State Psychiatric Information System. We examined how computers were actually being used in these organizations, how it was affecting individuals, several providers, payors and quality care providers, and so forth. The examples of valuable services, privacy abuses, and emerging new policies documented in the NBS study showed us the basic problems. What we lacked was the impetus for adopting meaningful new policies. It would be very valuable if we could update that in-depth case study work today. It was extraordinarily revealing both the informational dilemmas and the early pro-active good solutions that organizations were beginning to adopt.

The NBS report also provided two strong empirical inputs to the 1970s discussion. First, real episodes of people hurt by excessive data collections, data leaks, and forced disclosures of their health information were documented. We have had some good anecdotes along these lines at this conference, but I can assure you that a much more systematic collection and analysis of such material would go a long way to define the systemic problems and identify meaningful responses. I consider this vital as we approach new legislation, new regulation, or new association/organizational codes.

Breaches in Manual Records

Second, the NBS report discussed what automation was actually "doing" and "not doing" in the world of health information. Most of the problems of privacy and confidentiality were breaches still arising in the use of manual records, not in the computerized records. And the most common problems were-and are **still**—largely the result of people succumbing to pressures for disclosure that they should not succumb to, or of personal gossip and disclosure that would take place despite the type of records being used.

Clearly, major new developments can be taken into account in the past 20 years since the NBS report. The age of computer matching is here. The ability to create multiple databases and distributed communication capabilities is different from the big main frame, slave-terminal model of the 1970s. Today, we must also reckon with telecommunication information reaching everywhere, intelligent terminals on desk tops, and the development of smart cards. These create some new problems in defining rights and responsibilities. They also offer some attractive solutions separating and guarding particularly sensitive data not possible in the main frame environment.

In the NBS report, we also dealt with concepts that ought to underlie health data principles today. The list of 12 guiding principles that the NBS report ended with seem just as relevant today as when they were written in the mid-1970s. They offer some accumulated wisdom we can draw from and apply to the new environments.

Mobilizing and Energizing

Let me turn to the specific topic I was asked to discuss-the role of private organizations and associations. It is vital to the development and promulgation of good health information privacy policies that we recognize the political and policy importance of mobilizing and energizing the individual organizations and associations that are automating their records and creating the new information flows of the emerging national health care information system. They should be asked to bear the first and primary ethical, organizational, and legal responsibilities for grappling with these issues, and to bring major intellectual, financial, and experimental resources to this task.

Leaders of business organizations and even health care institutions do not wake up in the morning, look in the bathroom mirror, and say, " What can I do to protect privacy today?" Those issues generally become salient to organizations when they get into trouble-when they are worried that record subjects may not give them the information they need or when they fear that they will not be able to provide the care that they want to if information is cut off and that they will not be able to make money if regulations and legal liabilities impose heavy costs.

Organizations are generally institutions at rest. To move them takes advocacy pressure, the promise of competitive advantage, or the avoidance of regulatory/legal pain. In the real world, these are the things that make busy chief executives say, "Maybe we should create a task force. Maybe we need to protect our reputation for being concerned about our patients or our

customers or our policy holders." The real dynamics of organizational action to enhance privacy protection almost always stem from a concern by organizational leaders that they will not get as much individual information as the organization needs and wants for its own success.

If consumer and civil liberties and minority-rights organizations did not exist, we would have to invent them. Advocacy organizations are initially needed to advocate minority rights, individual rights, and values of protection of individuals and of social groups so that the attention and interest of organizational leaders will indeed be focused on these issues.

Money Spurs Action

Organizations and associations are spurred to action when they are preparing to spend giant sums of money on automation. And it is an article of faith in the privacy analysis that you should never, never look to either the computer or the systems people to be your privacy protectors. They are dealing with machines. From the policy people, they want frameworks and principles with which to guide their jobs in handling data, providing data security and so forth. But it is absolutely vital to distinguish between the value of policymaking in organizational life that comes from the interface between the organizational policy leaders, the society and the regulatory environment in which they operate-and the technical people who are executers of those policies, using a variety of systems techniques. There is a nice interplay between the best and the brightest computer people and the best and the brightest policy people. But the organizational leaders must tell their technical people what they are designing the systems to do; they cannot expect this to come from the system design.

Regarding the incentives and disincentives for organizations and associations to do anything organizations and associations need to be pushed into a proactive or responsive role. Usually a leading edge of organizations-5 to 10 percent-who, because of the organizational culture and the personality of the chief executive officer or some senior official, are interested in being innovative. Those are the organizations that take risks to consider new privacy and confidentiality policies-to create privacy task forces, bring in consultants, look closely at all the ways they are collecting and using information, see what kind of threats and harms may be involved, and so forth. Extraordinarily important in the development of good voluntary privacy policies is to recognize and celebrate such organizations if they do the hard work of trying to formulate and promulgate new policies and codes.

We may not agree with everything that these organizations/ associations do. We may not think that they set the balances in the right way But, if we ever expect the private sector and innovative government organizations to pioneer in this way, we should become accustomed to writing about them, praising them, and encouraging them. From the proactive policies of this 5 to 10 percent will come the next wave of 30 to 40 percent of bandwagon companies and agencies to say, " Gee, Aetna did it, IBM did it, Equifax did it, American Express did it, Citicorp did it; maybe we should do it too." The dialogue between the advocates of privacy and those proactive organizations represents a critical way for privacy rights to evolve and be protected in the real world situations in this decade and beyond.

Proactive Policymaking

Of course, law and regulation have an important role. But we need to recognize that most of the practical new policies and new codes on privacy will come from proactive policymaking of organizations and some associations. If we want to see this spread in the organizational world, we really ought to understand how we should and can encourage and celebrate those kinds of actions.

When we discuss legislation and regulation, several issues need to be addressed. In some situations, it is necessary to pass legislation or to regulate in order to provide the conditions for organizations to carry out proactive policies. In certain contexts, organizations need law to do the right thing. Also, sometimes law is needed to prevent organizations inside an industry or community from profiting from and violating privacy norms. Because these organizations do not pay the same amount or have the same system costs as organizations whose privacy policies incur costs and system encumbrances, the nonresponsive companies get a competitive advantage from ignoring legitimate privacy concerns. We may need to level the playing field so that the proactive firms are not disadvantaged in the competitive world.

In looking at the history of privacy legislation over the past several decades, I find that the policies worked out by proactive organizations

have provided the best framework for regulators and legislators in developing standards protecting privacy, Not that the "industry" or the organizations always recommend the same balances that the legislators will; but they offer examples of what is practical-what can work in a health care institution, a hospital, a clinic, an insurance company, or other information providers. By looking at these models, legislators and regulators can write the most practical and useful legislation. This is another reason for encouraging innovation and action from individual organizations and associations.

In the **1970s,** I served as research director for an excellent organization-the National Commission on Confidentiality of Health Records. Many organizations with representatives here participated in that activity. This nonprofit, voluntary sector organization brought together the Blues, the hospital associations, the social workers, the psychiatrists, the doctors, the ACLU, and others working cooperatively to identify the urgent needs of privacy and confidentiality. It expired at the end of the '70s because the medical records issue and the national health insurance issue vanished from the political landscape. This is an excellent example of the type of organization we should revive in the 1990s to bring together the private sector who need to be players and innovators in this area. This organization should be outside government, although cooperation with various state and federal agencies would always be fine. But that is where the creative role of the voluntary sector really ought to come in.

Collapse and Disarray of State Law

Everyone here has stressed the fact that state law is in a state of collapse and disarray. We need to put in place a lattice work of state and multistate statutes that will address the central issues of confidentiality, privacy, and access that have been discussed today, This is an issue in which state legislative leaders **are** interested and are ready to move toward enactment. The state level provides windows of opportunity, if we can bring together the interest group and party commitments to update state legislation as we move into an increasingly automated era for health records.

What about the federal level? As a privacy advocate and political partisan, I am delighted that we did not get federal legislation on medical confidentiality in the '80s and early '90s. In the Reagan-Bush era, it would have been dreadful legislation. If the Administration had anything to say about it, it would have been all disclosure and surveillance and no privacy. Therefore, many who kept the faith on federal privacy protection believed that their greatest role was to prevent legislation from taking place during the 12 years of Republican hegemony in the White House.

Now we have a new era. I believe the Clinton Administration and the Democratic Congress offer an excellent opportunity for genuine and powerful ideas about privacy and confidentiality as long as we also recognize the schizophrenic nature of the Democratic Party. One part of it is geared to social programs and solutions, and the other part is geared to a respect for civil liberties. So there is a battle over which half of the brain lobes of the Democratic Party will have the most to say about health care reform and privacy legislation.

Most of us that care about the privacy side ought to be briefing **Hillary** Clinton on how critical the privacy and confidentiality issues are in health care and health information policies. We need to make sure that policymakers **see** *from the beginning* that without strong privacy, confidentiality, and access protections, the American public, as data subjects, will not be happy and major political problems will surface if these issues are not addressed well.

What we really need is the equivalent of a Robert Reich from the labor and employment front to lead the privacy and confidentiality campaign in the health area. I would hope that someone like Donna Shalala might, because of her background and interest, be the person that would see the balance that needs to be struck between the health care interests and the privacy and confidentiality interests.

The opportunities are enormous to lay down critical foundations for privacy protection decades ahead of the large scale and expanded uses of automated health records that lie ahead. It is worth the effort of everyone here to join in that endeavor, understanding how much is at stake. ◆◆

Approaches to Privacy Protection: Policies and Guidelines

Pam Wear, M.B.A., R.R.A.
American Health Information Management Association

We have written daily to Hillary Clinton and to Donna Shalala. We have their Compu-Serve numbers now, so we can be a little bit more direct than the mail services. We believe that the environment is certainly right for health care reform and for addressing these issues of privacy and confidentiality.

Our organization consists of the professionals who have built most of the clinical databases in this country. We take the medical record as a source document and translate that health data record into most of the computer systems. Most of that information is very, very flawed. The translation guidelines are not good and the documentation is poor. *When we* think about re-releasing this information, we have even bigger issues than we would if we were releasing accurate information.

Our Guiding Principles

Confidentiality and patient advocacy are certainly our guiding principles. We are passionate about the computer-based patient record, and we believe we can enhance data quality and data integrity and better protect patient confidentiality in the computer-based patient record. We also believe in Madison Powers' "Nike Noah" concept: we just need to do it. It will be difficult to study and determine that it is a good thing to do, but I think that everything points to the multifold benefits of computerizing a lot of information.

Health Information Management (HIM) professionals always ask why; they want to know why you want it and what you want it for. I was pleased to hear yesterday that Mayo Clinic is such a shining example of a commitment to privacy It appears to really have its act together and does not allow inappropriate release of information to just anyone who might be interested. We are not the barriers in all of this; we are the brakes.

To address Florence Rice's concern, in California we developed a consent form that could be used as a model. The print is large and it cannot be copied. It states the reasons for the release, and it is time limiting. We put the patient's phone number on the form so we can call to double-check, to find out what original intentions were, and if those intentions still exist. We are hoping to move to a consent that is truly informed and not one that we have talked about a lot in the last day-a consent of coercion.

Personal or Impersonal

When we go through the release decision process, one of the most important things to keep in mind are two basic premises. As health information management professionals, our first guide in deciding to release something is whether it is a personal or impersonal request. The personal request is primarily for patient care. We believe in the longitudinal record; we believe that the social security number should be the linkage since it exists. Establishing another system would take a long time. We believe that, with appropriate securities and the patient password, we can maintain a secure longitudinal record.

Medical record professionals screen records when a request comes in and respect the patient requester that says, "Just send them information about my surgery. Do not send my mental health information; do not send my back injury information." So we already have mechanisms in place to respect and protect what individual patients wish. Those mechanisms need to be built into the computer-based patient record (CPR) so we can continue to do that.

The impersonal use is basically nonspecific to the patient's identity. Researchers would typically fall into the area of impersonal information requesters. They want something that is disease-specific or procedure-specific or symptom-specific. That information can be

provided, is provided now, and includes patient identifiers. We trust that researchers will not further use that patient identification. With the CPR we will be able to provide that information exclusive of the patient identifiers. In most instances, a researcher would have a difficult time making a case of needing the patient identifiers when they really want just the data. The same would be true for the state data commissions and even insurance companies. They can make their decisions based on aggregate use of information, not patient-specific information.

Of course, one of the reasons all these clinical databases have built up is because of the absence of the CPR in this country.

In many legal cases, an attorney is trying to prove that a physician did not follow the protocols that other physicians might have followed. The attorney might request that a hospital release records on, for example, all gall bladder cases. Then it becomes a privacy case because patient identity could be released. In that case we always let the attorneys know that we need consent; we will go to every single patient to release that information for the court case. Those are just some of the ways that we work very, very hard to try to service patient advocates and protect patient confidentiality.

Confidentiality of All Information

Some other things that we all need to keep in mind are certainly from the Institute of Medicine (IOM) report. It defined three different types of confidential information. Personally, I believe that no matter what type of information relates to health care, every single piece of information should be confidential. It should not matter whether the information is HIV, whether it is sexuality or whatever. So we need to keep it very simple and stick to that.

Anyone who is developing confidentiality policies and procedures should be aware of the IOM guidelines. It covers the least sensitive, the most sensitive, the traditionally confidential, and certainly the extremely sensitive. But keep in mind-it should all be confidential.

In theory, information is shared with the physician or the caregiver and is documented in the medical record. Of course, the original objective of the medical record was for patient care. Now, we all know that the medical record is written for the health care bureaucracy As a result, it is full of inaccurate, untimely, and incomplete information. We worry about privacy, but we should also worry about releasing information that does not have a lot of data integrity.

For example, how many physicians would record acute gastroenteritis instead of acute alcohol intoxication in a 14-year-old? Most of them will-to protect that child, for purposes of reimbursement, for the medical-legal, and of course, for subsequent insurance coverages. How many physicians really do record the AIDS diagnosis and related comorbid conditions? Some will not to protect the patient from the social stigmas we have talked about, from reimbursement problems, and from loss of employment.

Health care privacy legislation must eliminate these concerns so that accurate information can be documented.

How many physicians and care givers record information at the point of care? Is a history and physical that is written two months after the time of encounter really accurate? What about an operative report or a discharge summary? It really should be documented at the time of care.

How about authentication? Is authentication done two months or two weeks after? Is that legally permissible? We have really perpetrated a fraud in this country by allowing post facto completion of medical records. We truly believe that we need to move to the point of care documentation. The computer-based record will facilitate that.

How many patients have access to their health records to review them for accuracy and completeness? How many patients can relate their real history or their real social habits to the disease process? They do not, because they do not trust the system. Our goal in the Work Group on Confidentiality and Privacy in Legislation, a part of the Computer-Based Patient Record Institute, is to provide that trust not only for the patients but also for the providers and users of health data.

Organization of Organizations

The Computer-Based Patient Record Institute (CPRI) is an organization of organizations. It is very much the forum that Alan Westin talked about-it brings together both the public and private sector to develop answers to some of these difficult issues.

How many nurses write a progress note at the end of an 8- to 12-hour shift? How accurate is that? Can they remember all the patients and what they ate? Can they remember all their reactions to treatment? How many health

information management professionals abstract data from the medical record and translate it into coding systems without complete documentation? The physician might document myocardial infarction, but in a further review of the record and diagnostic imaging report, you find that part of the anterior heart was damaged. Does that have relevance? Is it relevant to the researcher or the outcome? It probably is. The good news is that most of the time that information is included somewhere else in the medical record and can be recovered even if the physician does not document it. But so much of the time we go by the information that is on the front of the medical record and in the discharge summary. It can be a lot more damaging if that diagnostic imaging report was not there for the treatment process or in the final analysis of the medical record.

In 1983, with the advent of prospective payment and the DRG system, we virtually destroyed the clinical database in this country. We began to code for reimbursement so our hospitals and other institutions could survive. Unfortunately, technology was not such to enable the vendors to provide us with the classification system for reimbursement. We should have been able to do both. At this point, we are encouraging the vendors to allow us that capability.

Simple things like an abstraction code, one of the data elements. for the state data commissions, was the source of admission. Medical record professionals do abstract that data and ask the questions: Did they come from the emergency room? Did they come from the physician's office? Did they come from a long-term care facility? That information frequently is not documented in the medical record. If the patient was in the physician's office and then the emergency room, which code to use is unclear. These are more examples of flaws in the database.

Creating Redundancy

How many physicians are treating patients based on information that is transferred from another facility or from the physician's office? Many physicians just simply do not trust that information, so they re-order everything and create redundancy and expense. For those that do trust that information, should it be in the medical record? Because clinical decisions are based on it, that information probably should be in the medical record, Yet this country's business laws preclude that and say that the facility owns the record. It owns only its information. This does not allow for the fact that we are trying to build a longitudinal record. Laws certainly need to address this process.

The other part is the health care principle of "if it was not documented, it was not done." This principle needs to be extended to the fact that if it is documented, it is accurate, complete, and timely. It is vital that we know this when we release a medical record for both personal and impersonal reasons.

The physician is a patient advocate. Can we fault that physician for trying to protect the patient? Can we build a computer system that will facilitate the accurate and timely information? Yes, we believe we can. We believe that the computer-based record must be accessible to all legitimate users. The major issues are all the standards development, educational resources, malpractice, policies, and procedures that will ultimately be used to implement the law in provider institutions.

A lot of regulatory barriers that will permit storage of electronic media appear to be going away. We continue to fight for this. Just this week, the Joint Commission on Accreditation of Hospital Organizations (JCAHO) let us know that it will not allow a computer authentication unless some mechanism demonstrates that the physician did indeed review that record. So making sure that we can create, authenticate, and retain the computer-based record in a new medium is a continual uphill battle.

Hundreds Have Access

The paper record is not confidential because hundreds and 'hundreds of people have access during the patient-care process. Hundreds of copies are distributed to physicians' offices, insurance companies, and places of employment. Patients are the ones that are most often denied access. They are the ones that need to participate in the building of their clinical database, encounter by encounter, and have the opportunity to review it.

Another data issue is redundancy. Not only do we abstract for state data commissions, we reabstract for all the registries and similar situation. This is another huge waste and another opportunity for error.

Who is working on these issues? CPRI is working on these issues. American Health Information Management Association (AHIMA) has just established, at the University of Washington,

a confidentiality clearinghouse to gather all the information and all the products currently being formulated from both standards groups, this privacy forum, and certainly CPRI and Workgroup on Electronic Data Interchange (WEDI) activities. That will serve as a resource to the Computer-Based Patient Record Institute. Many legislative issues need to be addressed. Who is doing something? The work group on CPR will review its final proposal for national legislation on confidentiality at its March meeting and put it out to you for input and reaction. This is a window of opportunity in the next 100 days of this administration to get that information to Congress. We have been in contact with Pete Stark (D-CA) and he is willing to put in that legislation. The bill he is currently sponsoring does not have a lot about confidentiality-it takes the simplistic approach that everything needs to be covered and that anti-health care discrimination reform should occur along with it.

We urge you to participate on CPRI-its next meeting is March 3 in San Diego. Once the policies are developed, then the technocrats can help to implement the security aspects. Physical protections need to be in place for the computers, both the software and the hardware, and cautions must be taken for remote access. Temperature and electrical surges and sprinkler systems and similar things need to be addressed, along with recovery mechanisms and redundant backup system.

Expectations of Legislation

WED1 is also working on confidentiality and expects legislation in Congress before this summer. Those technical advisory groups are meeting in Chicago, and you are welcome to attend. They also believe the social security number should be the patient identifier.

The state laws do not address internal access in a facility; policies and procedures ultimately determine what happens in a facility. Once we have the model legislation, we believe this University of Washington group will be able to help implement those policies and procedures. The ***In Confidence*** newsletter is where we plan to track the legislation and policies and the procedures.

Regarding yesterdays question about patient consent-I want to reiterate that we only release the portions that the patient wants.

We have talked a lot about data integrity and its importance. If things are to be encrypted, then everything needs to be encrypted and encoded, not just the super-sensitive information. We believe that the computer-based record will be more secure because now we have no way to control who peeks at a medical record. But with computer records, we will have audit trails. Anyone who logs on to an information system will leave a trail of what portions of the record were reviewed. So we believe that policies and procedures can then be enforceable.

We have talked about stun guns when you log on inappropriately or alarms that go off on those computer systems. All of the issues about passwords being changed frequently and about signing confidentiality agreements within a facility are very very important-and that applies to your vendors.

Guidelines need to be developed for secondary use; standards need to be developed on record content. We truly believe that the challenges of technology are new; but as Alan Westin pointed out, the issues are very much the same as they have been for the last 30 years.

So we urge you to collaborate with us, with CPRI, with WEDI, with this privacy forum, to provide all of the input that you can so we can get legislation through this summer. ◆◆

Approaches to Privacy Protection: Policies and Guidelines

Robert Gellman, J.D.
General Council
Subcommittee on Government, information, Justice, and Agriculture

Back in 1979 and 1980, we tried to create strong privacy protections in a fairly limited way. The effort failed for a variety of reasons not worth reviewing. As others have suggested, the opportunity has returned again, and I hope we can do something with it.

I agree with several things that Willis Ware said. The need for uniform rules has grown and will be even more intense as computerized systems come on line. I disagree with Alan Westin regarding the prospect for doing this at the state level. Medical records and medical care providers and patients travel back and forth between states. You cannot ask providers, insurance companies, and other payors to comply with 50 different state standards, even if they are very close. The nation needs a uniform federal standard.

Not Just Patient Rights

The problems here are-again, this is something Willis said yesterday-that we are not just dealing with an issue of patient rights. Patients need protection for their privacy interests and record keepers need guidance-they need to be told what to do. Basically few, if any, specific rules today tell them what to do in all circumstances. Record keepers need to be told, "This is what you can do, and this is what you cannot do."

Finally, I also agree with Willis that what is called for are a code of fair information practices and standard privacy remedies with suitable adjustments made for the nature of the data and the nature of the industry, The nature of those adjustments is where all the problems arise.

I want to discuss eight principles. Many are perfectly obvious and simple to do; many are extraordinarily complex. We can all agree on a one-line principle and then spend the rest of our lives fighting over the details. The details are what are important. So I recognize the difficulty and the limited value of the principles.

Appropriate Privacy

The first principle is very simple. All medical records should receive appropriate privacy and security protections. That is not the case today. Plenty of medical records float around and are under no legal or professional or ethical obligation to be kept under some kind of privacy and security standard.

The second principle is that record keepers and record holders should be required to prepare forma1 written statements of the fair information practices that they observe. Patients who provide medical information directly to record keepers and record holders should receive a copy of the statement and an explanation of those fair information practices upon request. This is the only way people can understand what is occurring.

Third, patients should have access and correction rights. This does not necessarily mean that patients should have access to all their records all the time. The issue is complicated with lots of different points of view. But patients can all be accommodated according to a standard uniform set of rules. Providing patients with the right to correct records creates lots of problems. The same principles apply-you come up with a set of rules with which you can live.

Essential Use of Information

The fourth principle, privacy and security protections for medical information, must recognize the essential use of the information in the treatment and payment process. It must provide for those uses in an efficient, reasonable, and controlled manner. This principle is significant because, in effect, it differs from an approach used with legislation 12 years ago. We can no longer separate the treatment and payment process.

Yesterday Mr. Brooks from Aetna pointed out that payment treatment, oversight, and audit functions are inextricably intertwined. They cannot be separated. The Zone 1 and Zone 2 concept from 20 years ago, which was probably accurate at the time, is no longer relevant. We have to give up on that fight, draw the circle bigger, and make the walls a little higher.

The fifth principle embraces the belief that some medical information is entitled to a higher than normal degree of privacy and security protection. It is all very nice to say medical information should be confidential. The word confidential means nothing. No medical information is confidential; all medical information is passed from pillar to post, all over the place. We need to look at who can get information, what they can do with it, and what rules are surrounding it. The sentiment that medical information should be confidential is totally appropriate, but it is not a principle that means anything.

We all agree that some information is more sensitive than others. We may have policy reasons, or political reasons, or other reasons for making the distinction. We have done so quite regularly in the past and we have discussed examples here—AIDS, drug use, psychiatric records, sexually transmitted diseases—take your pick My premise is that particularly sensitive areas cannot always be determined objectively

Providing for Sensltlve Information

Let me provide a good example. I know many people who see psychiatrists and speak about it all the time. However, I do not know a single person who has ever seen a proctologist; no one ever talks about that. It is clearly something that people think is sensitive and embarrassing, however you want to characterize it. Information that requires a higher degree of protection—and I do not know exactly what type of information that is-can be identified by law, by the record keeper, or by the patient. The question is how to provide for special treatment for identified sensitive information. We need to come up with a standard way of dealing with it and worry about what it applies to later. We need to provide a medical records system, be it computerized or otherwise, for treating this kind of information generically

The sixth point is the same thing from another perspective. For some patients, the entire medical record is entitled to a higher than normal degree of privacy and security protection. For example, I am sure that you cannot go down to the George Washington University record room and find Ronald Reagan's medical record sitting on the shelf. These records must be stored somewhere under lock and key, under restriction. The same thing is true for celebrities; the same thing should be true for hospital employees. Some people require a special kind of protection. Perhaps the medical care providers themselves can best determine whose records deserve special protection. It may need to be determined by law or by the patients themselves.

Specially protected records present problems, especially in cases of emergency when records are not readily accessible. These situations must be discussed and standards set.

High Barriers and Rigorous Procedures

The seventh principle is that uses of medical information not directly related to the medical treatment and payment process must be specially justified. As uses become more remote from treatment and payment, higher barriers and more rigorous procedures should be set. Many uses of medical information are required by law or practice or policy. We must distinguish among these and identify what they are.

Some uses of medical information for public health purposes are completely unobjectionable; many are provided for by state or federal law, and new policies should certainly not interfere. At the other extreme, we do not want law enforcement people walking into medical care providers' offices and asking for a record and total access to health data. We need procedures and rules. We need to limit the ability of law enforcement people and other remote users to ask for records. We need to limit the ability of medical care providers to turn over those records. And we need very elaborate and complicated procedures to accomplish that. The nature of- those procedures is something we need to work out.

The last principle is that every recipient of medical information must comply with the privacy and security principles. It is not enough to have principles-principles are developed and agreed to, and then ignored. People must follow the rules. We must have some kind of independent monitoring and periodic auditing to insure compliance. It is very nice to talk about a computerized system that maintains all these audit trails and keeps track of everything. But if we had a nationwide computerized medical sys-

tern, in any given day tens of millions of people or tens of millions of instances would occur where someone looked at those records. And if there are even 5 percent-I suggest that is a high number-5 percent of the accesses are for uses that are inappropriate, we are talking about hundreds of thousands of inappropriate uses a day. We need to devise a mechanism to serve as some kind of a practical barrier and devote resources to this.

Establish Sanctions

You cannot just have an audit trail that no one looks at. People have to look at it, know there are sanctions, and in fact, see people being sanctioned for inappropriate uses. All large information systems face problems of people surreptitiously getting records against the rules and, in most cases, nothing happens to anybody. It is highly institutionalized. Certain companies will sell you records from any of these systems. Price lists are published for illegal access to these systems; everyone knows they can get them and nothing happens. So in a medical records system, especially a computerized one, we need very effective controls.

Those are my tentative principles. I hope we can find a set of principles on which a large set of players can agree and then go to the much harder task of trying to translate those principles into some kind of workable, effective, efficient, and practical legislation that we can all live with. I hope this will be a project for the coming year. ◆◆

Approaches to Privacy Protection: Policies and Guidelines-Discussion

John Fanning, LL.B.
Senior Policy Advisor
Office of Policy and Evaluation
Department of Health and Human Services

Alan Westin, LL.B., Ph.D.
professor of public Law and Government
Columbia University

Pam Wear, M.B.A., R.R.A.
American Health information Management Association

Robert Gellman, J.D.
General Council
Subcommittee on Government Information, Justice, and Agriculture

■ **Participant:** For Ms. Wear, in regard to those business laws you referred to as barriers to the development of longitudinal records, you mentioned that these laws state, in part, that the institution owns the record. Do these laws state that the informational content from the records cannot be released or used to create longitudinal records?

■ Ms. **Wear: The** business laws, as you suggest, are based on the premise that the provider owns that record and the information in the record. The question becomes whether the provider can really validate information that comes from another facility Typically, most providers only provide on subpoena the actual records that were created within their facilities. Obviously we need to change the ownership of data laws. There are many questions about whether the patient, the provider network, or the governing board owns the data.

■ **Participant:** Underlying my first question is really the meaning of ownership. This does not necessarily take into account the informational content, as opposed to the medium. I am not suggesting that the institution release its ownership rights of the actual medium, but I am wondering if those laws actually restrict the information flow.

■ **Participant:** I am here on behalf of the National Committee on Vital and Health Statistics. I came to this conference expecting to understand how to better make a decision and whether or not we ought to be computerizing patient records. I really had no set agenda. I am convinced that most people here are in one of two camps. They are either absolutely committed to total privacy or absolutely committed to total free access and complete computerization of the record.

In my previous professional responsibilities, I computerized a patient record system at the University of Virginia, where we have one of the most computerized medical records systems of any hospital in the country. But, we made that decision based on a lot of information and an estimation of the potential benefit to the institution and patients in improved cost control, improved patient outcome, and improved quality of care.

I asked this question yesterday Mr. Westin, I thought your talk was brilliant. But I am also convinced that there is no such thing as confidentiality certainly not of an inpatient medical record. I have always had the illusion that maybe a primary care medical record, particularly in the hands of a single, solo practicing physician, might come close to being confidential. In an automated system, it clearly would no longer be a confidential record.

How do we decide whether the cost of that loss of confidentiality by computerizing the medical record is worth it? Do we have a burden on us to demonstrate an offsetting value to the individual or to society by virtue of computerizing those records?

■ Mr. **Westin:** I think the problem with an easy response to your question is that a lot of social issues are being thrashed out at the same time we are talking about how to automate the record and what the privacy guarantees are.

Technology now makes it possible for your sole practitioner to have a personal computer with intelligence and to segregate in his own or her own record system.

On the whole, though, automation makes possible the creation of something that is very good for health care. The problem-oriented record and Weed's concept of a new relationship between the care provider and the patient, using the record as a way to interact in more humane health care, is a situation where technology ideas, and better treatment come together.

Major advantages to certain kinds of technology applications need not be sacrificed in the interest of privacy and confidentiality. The task is to define them, institutionalize them, and surround them with the right kind of legal and ethical protections.

■ **Participant:** Do we have a burden to demonstrate the benefits or should we just accept the theoretical benefits?

■ Mr. **Westin:** Well, I think we have to demonstrate that, but in my case studies, that is demonstrable in real context.

■ **Participant:** I am from the Social Security Administration. I would like to present a dilemma. I have heard a lot about data collection and use of privacy for data **collection,** but the Social Security Administration needs access to medical records for entitlement. We service about 11 million beneficiaries and process approximately three million claims a year. We request **approxi**mately 14 million medical records to process these claims.

Our dilemma is that while the claimant gives permission to get records to process his/her claim, the provider community requires that, each time we go to them, we have a specific document that indicates permission to access the patient's records. That generates millions and millions of requests and adds a great deal of cost.

We tried to pilot very different approaches to secure privacy of the record by doing or proposing demonstration projects with a signature file record. The release would be in our records and the provider, based on that release, would give us the medical evidence. Very few providers have wanted to participate in this pilot test.

We are wondering about alternatives or other ways of doing this. My colleague addressed voice release encryption, but this does add to the cost.

■ Mr. **Gellman: The** old model of doing things with consent is a nice model, but you point out the attached expense. At least in talking about ways of making the process efficient, you need to look at alternatives. The notion of passing consent forms back and forth in order for everyone to have the piece of paper may not be necessary If you tell patients what is occurring-i.e., I give you my insurance form and say you can get paid in this fashion--consent is either implied or expressed. With a clear statement of information practices, patients can be told that. It may be possible; it is part of the same process.

I made that point about treatment and payment being the same thing now. No one is willing to treat you any longer without knowing how they will be paid; we have to recognize that reality You may have to change the system. If I come in and give you my Medicare number, that is enough of **a consent.** I am told what the rules are, and unless I tell you expressly that you cannot do it, then we can all assume that is a way of doing business.

That has some problems, but some costs **are** involved with doing it other ways. I think it is something that must be considered. ◆◆

Ownership, Uses, and Dissemination of Health Care Information: Who is in Control?

Vincent Brannigan, J.D.
Professor of Law
College of Engineering, University of Maryland

In the College of Engineering at the University of Maryland, we are trying to build an understanding of technology and law and how it really works at the nuts-and-bolts level. So today I will describe the history of privacy and why we are having this problem on a operational level, and the regulatory effectiveness analysis tool we have developed to try to address it.

The existing Privacy Act for the federal government and its records will affect anything that is going to happen nationally in health care records. Agencies "shall establish appropriate" safeguards to insure security and confidentiality. Now, this is a wish list if there ever was one. In fact, I have given many lectures to large groups of medical information people in the federal government who have never heard of the Privacy Act.

Conflicting Models

Let us begin with the oath of Hippocrates. Our problem' is a conflict between two models of medical privacy. In the 19th century we developed the ideas of doctors in offices and paying patients having privacy. This is an extension of the household privacy mentioned by Hippocrates. But hospitals are derived from charity institutions where patients never had any expectation of privacy. Patients were things to be operated on; they were subjects for research. They were even, if you remember Marquis de Sade, subjects for entertainment; they had no privacy. So we have a conflict between two models. Medical privacy was not a traditional obligation of hospitals; thus, it did not become part of the contract between the patient and the hospital.

In the 20th century, hospitals began treating middle-class paying patients. The patients thought they were getting privacy; and the hospitals thought they could still run things for administrative convenience. This is where the problem originated. In the 1920s, the development of surgical records in the United States was for hospital quality control, not for patient treatment. Records were used to figure out which doctors would be allowed on staff. Documenting the incompetent prevented them from practicing on the hospital staff and making money

Hospitals continued to treat patient data with the same attitudes they used in treating charity patients-a lack of patient confidentiality because it was not administratively convenient. But changes in medical therapy helped expand records. Insurance and cost control demand more exact medical records, and computerized information systems made provision of those records easier for both authorized and unauthorized observers.

My argument is that data was protected by accidents of hospital structure, not by deliberate action. Medical records in hospitals were cryptic—hand-written in single copy-and you could not find them for a legitimate purpose. That is what protected your privacy-the absolute confusion and chaos of the typical medical records room.

Three Kinds of Privacy

Now the law essentially recognizes three kinds of privacy. Locational privacy protects a specific place against intrusion. That is why we put doors on bathrooms. Everybody knows what you are doing there, but they are not allowed to watch you do it. That is locational privacy, and it is mentioned specifically in the Constitution.

Behavioral privacy protects the individual's right to engage in specific actions, like using contraceptives, and limits the abiity of others to prohibit the behavior. Some people use the term "autonomy; I use the term "behavioral privacy." An example is the contraception/ abortion decision.

Informational privacy protects the individual's interest in personal data, including medical

records, and is created by statute and common law. The Supreme Court has recognized in the *Whalen* case [*Whalen* v. *Roe,* 429 U.S. 589 (1977)] that disclosure of private medical information to doctors, hospital personnel, insurance companies, and public health officials is a central part of modem medicine, even when the disclosure may reflect unfavorably on the patient's character. They, therefore, found no constitutional right to prevent government from *collecting* certain kinds of data. So requiring such disclosures to representatives of states does not automatically amount to impermissible invasion of privacy. I find this quoted numerous times in government documents supporting data banks, but they never go to the rest of the decision, which puts strict limits on disclosure of data.

No federal court has ever allowed a compulsory collection of data that was available on-line in a computer system. In both the *Westinghouse* [*United States v. Westinghouse Electric Corporation, 638* F2d 570 (3rd Cir. 1980)] and Whalen cases, the data, insofar as they were ever handled on a computer system, were in a secure, off-line environment and were not allowed to be kept on the system. And in the *Whalen* case, a tiny handful of people were allowed access to the data. So computer people see the *Whalen* and *Westinghouse* cases, which allowed the government to collect the data and process it, as indicating that no privacy protection is strong enough. In fact, what they allowed is a very, very limited, narrow kind of data processing under the constitution.

Under the *Westinghouse* case, the leading case on this subject, the medical records privacy factors looked at were the type of record requested (medical records are a type), the information the record does or might contain, and the potential for harm in any subsequent nonconsensual disclosure. The latter is the single most important factor that the court looked at-the injury from disclosure to the relationship in which the record was generated. This is particularly true for psychotherapists. Other factors were the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether an express statutory mandate was articulated. In other words, what is the rationale and support? These *Westinghouse* factors should be the guideline for anyone analyzing how the legal system might look at privacy.

A Design Criterion

I believe that privacy is a design criterion for systems; it is not enough to be in compliance with current law. Systems have to be developed that are secure and flexible enough to cope with foreseeable changes in the law. This is the advice I give. Developers simply doing what everybody else does will not be good enough in the future-we will call that the Zoe Baird test. A theory of privacy is needed to satisfy the *Westinghouse* factors. This happens to be a theory I have developed with Dr. Berndt Beier in Germany in our international work. Our argument is that informational privacy is desired because of the way information might be used or perceived by others.

We developed the concept of the "affected person" and the "reference group." "Affected person" is an exact translation of the German term used in the data protection law. The difference among individual's concerns about disclosure of medical information depend on how the reference group might act or react towards the patient.

The goal of individuals in the area of informational privacy is to protect themselves from the real or perceived adverse consequences of the data becoming known to the reference group. A person who would not be subject to adverse consequences can be defined as normal. In other words, whatever the information, if you would not be subject to adverse consequences, you define yourself as normal.

Of course, an individual's concern for medical privacy depends very much on whether the particular medical information is indicative of a "normal state." The purpose of informational privacy is to allow individuals to project themselves as normal and, thus, avoid adverse consequences, even if in reality they are outside the normal range. Privacy is operative, therefore functional, to protect the individual's claim of normality

So against this conceptualization, what is the problem with the medical model of privacy? For many patients, the immediate family or coworkers are the key reference group. They do not care whether people in Austria know. However, they may go to Austria to protect privacy In the example yesterday, however, where they sent the Dictaphone belts 500 miles away for transcription-people go 500 miles away for psychiatric help for that reason. So why are they surprised when they send the belts only 500 miles away, with no other protection, and the transcriber recognizes the patient? In other words, a system analysis would have shown that was a fallacious method of protection.

Outside the Private Sphere

Prohibition of disclosure to this reference group is often the goal of informational privacy; but this group has traditionally been considered within the private sphere in health care. This was the problem with the remarks of the gentleman from Aetna. He assumed that the employer was within the zone, whereas the employer is the precise person the individual does not want to have the data. Similarly, you may want to keep the information from your mother or your sister, not from some researcher in Austria. Your worry is whether people in your reference group can get access to the data. The health care system is concentrated on preventing disclosure to strangers, when the real risk is disclosure to the reference groups.

I will give a personal example. I am married to a physician computer expert. I cannot tell you the number of times physicians have left messages **containing very** sensitive data on our telephone recorder. I cannot tell you how many times I have worked with people in hospital laboratories who have fax boards built into the system so they can **autofax** results to a fax number provided by the doctor. Where is that fax machine? How is that machine protected? Is it also the one used for billing and everything else?

In regulatory effectiveness analysis, we try to measure compliance with the technological **regulatory** system. By examining the public policies, the legal structures, and the technical tools involved in the regulatory system, we can discover discontinuities that can result in noncompliance.

Regulatory effectiveness analysis starts with a paper audit. In other words, we look at the security system on paper. We are still working on the techniques of doing the field study We first worked on government hospitals. The regulatory effectiveness on this analysis indicates the level of privacy being mandated by compliance with the regulatory system. You also must look at the policy goals, legal structures, and technical tools.

Public policy is a narrative statement of the goals to be achieved by the regulatory program. We do not yet have a straightforward policy statement available, but conflicting multiple policy goals are acceptable. **In legal structures, regu**lation requires a mechanism to enforce the social will on individuals who would not otherwise comply, Regarding technical tools, every technology has a distinct and often limited set of technical tools available. This includes encryp**tion** and all the different methodologies for protecting privacy.

Interlocking Requirements

Public policy legal structures, and technical tools have interlocking sets of requirements and capabilities. Requirements are the preconditions that must be satisfied by other components before a component can function. Capabilities are the ability of a tool to satisfy the requirement of the component, and a discontinuity is where they do not match. When what you have in one component does not match a piece in another component, we call that a discontinuity. It can exist among the components even when the individual component is properly designed; that turned out to be the most interesting result.

We are looking both separately and together at the public policy the legal structure, and the technical tools involved in a particular information system. You often find that the **discontinuities** are between the legal structure and the technical tools, or between the legal structure and the public policy. In other words, we believe the problem comes, particularly in the medical computer area, because public policy is made by politicians, legal structure is made by lawyers, and technical tools are made by engineers and computer scientists; and they do not use the same words in the same way

A Structure of Lying

These people use the same word in different ways, and they he to one another. For example, the management in a hospital lies to the doctors about why they are putting patient information in the computer system; the information people lie to doctors and to management; and the management lies to the computer people. Everyone takes comfort in these lies. But the ones who get forgotten by the system are the patients, because they are not participants in the structure of lying.

I cannot tell you how many computer directors have said, "Well, we have someone's signature on file; we know who is responsible." We call this the responsibility structure-a defined individual is assigned the obligation of preventing injury, with potential penalties if they do not. That is the structure-we are going to make someone responsible.

Well, responsibility structures have requirements if you are going to use responsibility. For example, you must define the individual who is

sanctioned for the default. In a number of cases, you cannot figure out who changed a computer record or who did something similar, because nothing attached to the record meets your standards for defining who should be sanctioned.

The default, the injury and the sanction must all occur in a reasonably short time to hold someone responsible. It is meaningless to say, "Well, 10 years ago. .. where is that person? We are going to hold them responsible."

The sanction must be sufficient to deter the unwanted conduct. In the ***Behringer*** case where people failed to secure the charts, no one suggested that the responsibility system include disciplining high level people who make the system design decisions. Some low level clerk is always the one fired.

Tracing the Default

The responsible individual must have actual control over the default. This is perhaps the most difficult factor in the privacy area: the injury must be traceable to the defined default. This is why we do not have enough lawsuits. You might be able to track, as in the ***Shady Grove case*** in Maryland, which person told your mother that you have **AIDS—that** might be possible. However, it is much harder to prove you did not get a job because someone accessed the system. So the number of lawsuits does not mean anything in determining the number of injuries.

In precaution structures, the policymakers have determined in advance that a designated individual has the obligation to carry out the specific acts, and they have determined which tools must be implemented. A defined individual must carry it out, the action must be specified, and a method to determine that the action has been carried out must be specified.

Precaution and responsibility are two of the most important tools. The difference between them can be explained using the example of a government family planning program. Under the precautions approach, you make people use contraceptives; under a responsibility approach, you file paternity suits. It all depends on how good you are at finding people, nailing them, and so forth.

These are both legal structures, but they have different advantages and disadvantages, given different environments. If you do not have the right technical tools to match your legal structure, the discontinuity renders the whole system nonfunctional.

So the key question for the regulatory effectiveness analysis is this: Do legal structures exist that properly implement the technical tools, and do the legal structures and technical tools, acting together, correspond to the policy statements contained in the Privacy Act (actually, in many cases, the Privacy Act notices)?

Don't Get **Sick**

I work mostly with hospitals, and I work my way outward from the machines in hospitals. My experience reminds me of the FDA's motto on medical devices: Don't get sick. You must simply assume, in most hospitals, that any piece of data you give anybody is available to anybody with sufficient interest in the system.

I will give you just three examples. First, does your hospital have a policy statement prohibiting doctors from using cellular phones? If you do not prohibit use of cellular phones, you have not even started thinking about privacy. I cannot tell you how many doctors I have seen and heard on golf courses talking about patient data on cellular phones. People sometimes tape the conversations. It is illegal, but people do it.

The second example is the use of fax machines around hospitals with absolutely no security and the other end. This is a problem before we even get to the computer system itself.

Finally, the Department of Veterans Affairs says in its Privacy Act notices-formal notices that go in the Federal Register-that your data is protected by a "need-to-know" system. The one line that says that nobody gets access to data who does not have a need to know sums up the entire philosophy However, no operative technical tool defines what constitutes a need to know.

Every hospital I have looked at has sacrificed dealing with the need-to-know issue to avoid ruffling the doctors. It is not impossible to install such a system; it simply takes will in many cases. You just have to change people's perception of reality

Study the Titanic

I have written a whole lecture about how everything we need to learn about technology regulation we can learn from studying the litanic-remember, the Titanic complied with all government regulations. But even better for the medical computer community is the **Hinden**burg. When people say, "But we have not had any lawsuits yet," the answer is very simple.

Before the Hindenburg crashed, a paying passenger had never died on a zeppelin. After the Hindenburg crashed, a zeppelin never had another paying passenger. Ask the people who make nuclear power plank. You can live in a fool's paradise if you do not sit down and do the hard work of figuring out how to satisfy the conflicting goals of privacy and access.

I am a little distressed at the lack of privacy analysis. When I look at privacy protection in hospital systems, the hospital directors are very proud that they are putting passwords on the system. Under the Buckley Amendment, we have much more privacy over our student records than almost any hospital has over ik medical records. And let me tell you, medical records constitute a heck of a lot more concern than whether a student gets a C in my technology law class.

So I think that we have to go someplace forward, do much better than we have been doing.

Discussion

■ **Partlclpant:** What is your opinion on tying this whole longitudinal-i.e., cradle to grave—record to the social security number as the key identifier.

■ **Mr. Brannlgan: The** Indian Health Service does cradle to grave-womb to tomb, they call it-studies on people, many of whom do not have social security numbers, so they do not use it. Patients get all their health care from within one system. I think Rutgers had a case recently on social security numbers that said you cannot post grades by social security number. Social security numbers are totally insecure. At the University of Maryland, we will issue anyone a different number if they do not want to use their social security number. That is a matter of policy.

So I have the feeling that we may be better off with a national health care identifier number, which might at least protect against some misuse. But I have not analyzed it.

■ **Partlclpant:** How do you crank the consumer into this process, into this decisionmaking process, particularly at the front end, but also at the back end? In other words, once you have a process, how do you get a complaint system going?

■ **Mr. Brannlgan:** I just finished a project for the American Bar Association that introduces consumer protection law into Bulgaria. This is starting from ground zero. How do you get consumer protection started? Essentially it is like building a bridge. On the one side, you can use mass entities that are surrogates for consumers. And on the other, you try to reduce your transaction costs sufficiently to allow individual consumers to have meaningful controlling complaints in the system. Sometimes you compromise. For example, in Europe, they rely much more on group consumer actions than they do on individual actions.

A great deal depends on access to the system-things like attorneys' fees or people being available. It is always possible to do; it is not always worth doing. You may sometimes be better off with group control over rights, rather than individuals; that is a very hot debate among consumer science professionals.

■ **Participant:** It seems to me that the probability of detection is an important factor in whether the sanction is realistic or not.

■ **Mr. Brannlgan: In** the responsibility structure, the sanction has to be sufficient. The probability of detection is included, in the written work, under one of the other categories that deals with the ability to connect. That depends on the probability. For example, we do a lot of work on oral contraceptives and breast cancer, but you cannot figure out which person got breast cancer from oral contraceptives. In other words, using responsibility structures is very difficult in those areas.

What we are doing is developing these tools generically enough to then contribute something to the national debate. ◆◆

Ownership, Uses, and Dissemination of Health Care Information: Who Is in Control?

J. Michael Fitzmaurice, Ph.D.
Director, Office of Science and Data Development
Agency for Health Care Policy and Research

I would like to express my appreciation for such a fine conference to Harvey Schwartz, who is responsible for confidentiality and privacy issues in my office. I would like to also thank Joan Turek-Brezina, who not only chairs the Privacy Task Force but has done an inordinate amount of work in helping make this conference a success; and the person who has really put out a lot of work, Rene Kozloff of Kunitz and Associates. For all the fine work that they have done, I would just like to express my appreciation.

My message is this: We are researchers. Trust us, but under binding conditions that minimize the potential for harmful impacts on confidentiality and privacy and under conditions that give confidence to the public that their trust in the health care system is warranted and well placed.

Make the Data Better

The Office of Science and Data Development has primary responsibility for developing improved medical effectiveness data sets and better methods for analyzing those data sets, in response to a congressional mandate. Congress told us to facilitate the development of practice guidelines, to undertake medical effectiveness research, and to recognize the limitations of the data available for medical effectiveness research. Congress said: "Make the data better."

In our authorizing legislation, we were told to develop uniform definitions, common reporting formats, and standards for patient care data. In 1992, we had an Automated Ambulatory Medical Record conference, one of our responses to the legislative mandate. The conference goal was to discuss the feasibility of a cooperative organization of computerized automated ambulatory medical records systems that would routinely supply. data to researchers on request. The purpose was to analyze the important issues and questions before considering such organization or collection of data. To address questions of interest, group sessions led by moderators focused on several areas. Two of these were medical/legal issues, moderated by Vince Brannigan, and implementation of a central national data source, moderated by Dale Schumacher.

Under medical/ legal issues, confidentiality, and security, we learned that energy is often devoted to assigning blame after a breach in confidentiality rather than having in place precautions necessary to keep problems from happening. Security must be viewed in terms of gradations, and not as an all or nothing proposition. For example, you can take out the ICD-9 codes from a 'record, but a diagnosis can be discerned almost as well by inspection of procedures recorded or of medications administered.

Privacy is Expensive

Further, the penalties for violation of privacy are not well known, nor are they strongly enforced. Privacy can be a very expensive part of the incremental cost of data collection. These points came under discussion in this work group. Cost effectiveness and cost benefit issues are of primary importance. The group posed the question: Is it technically possible to have a secure system in a network situation? The group did not have the answer; it said only that the most vulnerable areas need to be identified and the possibilities of leaks rectified.

Data ownership issues were also addressed within this same group. In legal terms, data ownership is difficult to ascertain. The patient's experience with medical data privacy and ability to access his or her own medical records depend very heavily on the nature and structure of the health care organization-managed competition, fee for service, Medicare, Medicaid.

The participants felt that the issue of who owns the coding system that makes the data

valuable is more important than the issue of who owns the data. We would probably not find unanimous agreement on that because of the feeling that the one who owns the data can always destroy the data, subject to legal and regulatory concerns. We have all heard of legal rulings that prohibit destruction of tapes of office conversations and E-mail archives at very high levels. So we see that the one who owns the data cannot always determine what can be done with the data.

Discussions focused on which users of the central data source need to be licensed. The concept of ownership, as discussed previously, must be considered within this framework. For example, if a highly marketed word processing program or a coding system had an ownership stake of some sort in every file created by users, how would this be handled and regulated? Consider all the Word Perfect or MultiMate files that are out there. It was agreed that legal advice was imperative on this.

A work group on implementation of a central data source felt that the following question needed to be analyzed: What are the incentives to share data for owners of automated ambulatory medical record systems? The work group said that contributing to a central data resource, a reimbursement for the data collection, and protocols for sharing data and publishing manuscripts were critical issues. Data collection has a cost. What are the resources used in bringing the data together? Under what conditions can it be used for publications? Issues related to **governance** of this central resource include data ownership, data use and data release policies, and public access to data. Decisions must be made on whether oversight of the resource should be public or private, and what role the stakeholders need to play. Legislation or regulation of these points may need to be developed.

Generally, no consensus or agreement was reached on the current ability of automated ambulatory medical record systems to support medical effectiveness research. Concerns were raised about the lack of data uniformity, the lack of record content and element definitions, and the lack of adequate outcome information. Often, you need to follow the patient after the patient has gone to an ambulatory source of care, to obtain patient outcomes from an acute hospital episode of care. Despite these concerns, the group agreed on a general recommendation to develop a systematic, planned, and phased effort for implementing a central data resource.

Linkage and Sharing-Important Issues

Data linkage and data sharing were very important issues. Technological advances and increased health care information demands by insurance companies, by utilization review organizations, by providers, and by researchers and others appear to be challenging traditional objections to data linkage and shared access across government and private databases. The sharing of identifiable databases for statistical purposes has potential benefits, including the enhanced effectiveness of currently existing databases by creating linked records containing more information than any single component database. This can occur without additional field collection costs, so there are economic benefits. These benefits can make enriched data sets feasible. Examples include patient histories, cohort studies, disease registries, highway injury files, mortality and morbidity statistics, and death indices, each with its own confidentiality and privacy concerns.

Record linkage can help track out-of-facility use of services, such as inpatient and outpatient use, without the expense of large data collection. Linkage provides the ability to assess the bias of single institution studies or the bias due to a focus on the part of a single institution. In many cases, getting as broad a coverage as you would need to avoid this bias is impossible.

Now, how should potential reductions of time and effort of data providers and of the cost of desired data be taken into account? Who will have access to the linked data sets? Who should decide? If precise linkage is the problem, what about statistical linkage where you take away the social security number or the name of the patient but you link on other variables?

For that, I am reminded of a story about a substitute teacher who came into school to teach biology. For the first two hours of the period, she went over birds-wrens, robins, eagles, and thrushes. And at the end of the two hours, she said, "Close your books and take out a note pad, a pencil, and paper. We are going to have a **test**— I talked with your teacher and it will count for 25 percent of your grade. The test is this: We have reviewed all these birds. I am going to cover up the tops of the birds. By looking at the birds' legs, you must tell me their names." The class was a little upset. While they put their papers together and got their pens ready, one boy stood up and said, "I don't think that is fair-it's a horrible way to teach biology You didn't tell us that you were going to give us a test that counts

for 25 percent of our grade. It is entirely unfair, and I don't think we should do it." She said, "Young man, what is your name?" He reached down, pulled his pants leg up above his knees and said, "You tell me."

Depending on Data Development

Technology and research planning continued operation of high quality medical effectiveness research, and AHCPR research into cost, quality and access all depend upon data development. Data development depends upon the public confidence in the ability of AHCPR and of the private sector to protect privacy. The Privacy Act of 1974, which Mr. Brannigan quickly reviewed, is a government-wide records management statute with relatively generous disclosure provisions.

The AHCPR itself is constrained, or you might say benefited, by a confidentiality statute in its authorizing legislation. The practical effect of this statute is to lead AHCPR, when collecting data, to make an agreement with those providing it-an agreement that governs further use of identifiable information. The purpose for which it was supplied, and for which the respondent is told, defines the allowable use of the data. The strong confidentiality protection afforded by the statute-and I believe the National Center for Health Statistics (NCHS) also has such a statute-permits a legally effective agreement that the information will not be used for anything but research. This benefits the agency and encourages data holders who are concerned about the privacy rights of their patients or of their beneficiaries, or who are concerned over data about themselves, to provide data to AHCPR. It means that under the Freedom of Information Act, you cannot obtain that data from us.

Fundamental to research is an agreement between the subject of the information, as gatekeeper, and the researcher about how the data generated by the research may be used. This issue was recognized in a 1991 General Accounting Office report that analyzed hospitals' use of automated medical records, and also by a recent American Medical Association Board of Trustees report that urged that stringent security procedures be developed to preserve patient and physician confidentiality.

Who Validates Research?

Regardless of the level of automation, another possible conflict between openness and confidentiality arises when scientific data are shared: Who validates research that uses confidential data? Suppose I put out a research article, and it has a striking finding. If you come to me and say, "I am not sure that applies. I would like to look at your data." Can I say, "I am sorry you cannot look at the data"? Should a validation committee somewhere be empowered to look at confidential data to validate scientific information?

Continued operation of high quality medical effectiveness research programs and health services research programs depends on public confidence in the ability of AHCPR and the private sector to protect privacy. That is important enough to say again. The increasing importance of medical effectiveness research often involves research groups at more than one institution, such as our patient outcome research teams. We have 14 such teams, each receiving a $1 million a year for five years, to look at what works in the community's practice of medicine. For that, you need large databases. But this large-scale, multi-institutional-based research often requires a diversity of methods for its conduct, and different conceptions of data and how to analyze it. Frequently you need to bring in people from various disciplines, often people outside the university When these unique databases exist, there are pressures for sharing them. The economics are overwhelming-it is expensive to collect and clean a large data set twice.

In the area of data sharing,. are data from funded research controlled by the investigator, the research institution, or the funder? What are the valid or acceptable secondary uses of the data, and who decides that? In collaborative scientific research with specialized scientific roles, a written agreement prepared at the project's outset should describe who controls the data, who is responsible for their correctness, who insures that legal and professional requirements of confidentiality and privacy are met, who orchestrates the sharing and who is answerable to questions and criticisms. The agreement should include the extent to which it governs the rights and responsibilities of investigators to review, verify, publish, and subsequently use and share the data.

Researchers can ask their subjects for consent not only to current research but also to the use of data by other researchers with appropriate conditions. Data suppliers and data recipients can craft agreements by which prior arrangements can be honored; in fact, it is a necessity. In addition, they can work out such issues as appropriate credit and the allocation of the costs of sharing data.

Legal Standards and Negotiations

Appropriate agreements should result from legal standards, from professional principles, and from negotiations on a case-by-case basis. These negotiations must include rigorous airing that determines the genuine needs for confidentiality Certain measures to be required must maintain confidentiality and provide binding assurances to subjects, hosts, and sponsors of research using patient care data.

The fine track record of researchers in safeguarding the confidentiality and privacy of patient care data and in providing useful research findings is a firm base that allows us to build a reasonable set of conditions for moving this research forward. In the process of patient care, patient care data is controlled by the patient, the health care provider, and subsequently, the payor, the researchers, and others. We have had little to fear so far from the use of confidential data by responsible researchers.

I agree with Larry Gostin who said earlier that public benefits must be made clear and be directly linked to the data collection. The development of reasonable and binding conditions for data use by researchers-conditions that balance the public good with patient care data and with the private good of avoiding harm to the individual-will serve the good of all. A fire engine must be able to get to a fire even if it must cross over property to which I have individual rights. The fire engine must also be able to make timed runs to and from different locations, some across my property, so that the fire company can determine which engines to send out in case of a real fire and where to locate the fire station.

Discussion

■ **Participant:** From your perspective, Dr. Fitzmaurice, could you comment on Robert Gellman's suggestion that privacy of medical records should differentiate between records of different degrees of sensitivity. He was the only person that articulated that point of view, although a number of people suggested that privacy protection ought to be across the board for medical records, generically, rather than for particular categories in different degrees.

■ **Dr. Fitzmaurice:** I mentioned different levels of confidentiality or privacy for different portions of data. But often the sensitivity or the damage depends on the kind of data in the record, what it shows, and how it is identified with the individual.

I support linking patient care data across sites and over time, so that the medical effectiveness researcher has a longitudinal database to find out what works-when you undertake a procedure here, what is the outcome six months or six years from now. The researcher does not have to know who the patient is; the researcher only has to be confident that someone, perhaps the institution itself, has linked the database together.

Perhaps we need a regional organization in which everyone-the local and state governments, the medical authorities, and the patients-has confidence that confidentiality will prevail. As long as the records are linked together, you can strip the identifiers and give them to the researchers. So under that guise, I would not strip out a lot of the confidential information, as long as it cannot be linked back to the individual patient. ◆◆

Closing Remarks

David Flaherty, Ph.D.
Professor of History
University of Western Ontario and
Visiting Scholar, Woodrow Wilson Center for Scholars

I want to join in thanking the organizers for putting together a very compact and, indeed, dense conference with a lot of good exploration of these matters. I also want to congratulate the paper givers.

I will not comment on research uses of personal information. I am sometimes thought to be an apologist for the research community, but I really do not think that research uses of personal information in the medical field are a particularly sensitive matter from a data protection point of view. This is not a particularly privacy-intensive issue.

My comments regard insuring privacy and data protection in providing health and medical care. What I have heard in the last couple of days has largely reinforced my own views. I hope my remarks and those of the previous commentators will be taken as advice to the Task Force, which I urge to get going with what it ought to be doing.

Enforceable Legal Rights

The discussions made clear the essential need to act at the federal and state levels, if possible, to provide enforceable legal rights to privacy and data protection in the medical and health field. That largely means insuring fair information practices-fair *medical* information practices, as you have heard ad nauseam-for health and medical records, whether in hospitals or in physicians' offices. I am as concerned in my comparative work in various countries about medical information in doctors' offices, where much of the information originates, as I am about what is in hospitals.

Data protection problems exist for both manual and automated records systems and both need to be legislated. We can expect both to coexist into the future, given the extent to which a paperless society has not been produced for us in other aspects of our lives. We can anticipate multiple systems to coexist, even in the same settings. At a recent Office of Technology Assessment (OTA) workshop on the computer-based medical record, we received information about five separate competing or complementary automated systems within the Duke University medical system. I suspect that will continue into the future.

Fair information practices must be built into the software and security regimes sold by vendors. That would make an enormous contribution to insuring fair information practices. People who design software ought to be encouraged to think about informed consent, for example, and other kinds of notices that people should be given in a meaningful way. Take the standard fair information practices most clearly set forth in the United States in the Privacy Act of 1974 and put them into the software used to run these systems. What you will end up with is the enactment and implementation of principles and fair information practices to insure medical privacy, generally. I certainly endorse the principles that Bob Gellman read to you; they cover things fairly clearly

Flashy Versus Basic Issues

Let us distinguish between the flashy issues, such as those dealing with AIDS and genetic testing, and the basic issues in data protection. I want to remind you of a couple of these, most of which were talked about previously.

Patients should have complete access to their health and medical records. Some qualifiers are usually put in place, but this is the mid-1990s when we have an increasingly literate population. My premise is that records should be open.

One of the most important aspects of insuring meaningful data protection is the problem of staff training in medical offices and in hospitals, particularly through development of detailed

manuals and monitoring of staff performance and commitment to duty.

Audit trails have been mentioned a couple of times. Fortunately, the technology provides a capacity to even monitor the entering of key strokes on computerized systems, so you can actually deconstruct a medical record and how it was put together. The technology is of great assistance to us. You essentially have auditing regimes in which auditing takes place after every interaction on a system. Security officers only need to look at data when blips occur, oddities occur in practice, or when complaints occur about unauthorized access to a person's information.

As a privacy advocate, I am keen about the segregation of sensitive records, when necessary whether they are American Express, hospital, or medical practice records. Celebrities, people with AIDS, or even notorious people should have segregated medical or health records so that they are not easy to access for illicit purposes.

Minimizing Intrusiveness

One of the basic principles of the Privacy Protection Study Commission's 1977 report is the centrality of minimizing intrusiveness in people's lives. That is the thing that is always forgotten here. These days, I often regard a hospital as a record generating system. That is all it is-just a big place to house paper and computer records. We need more agreement on the nature of a patient record and what should be in it. There should be more data purging, file purging and data destruction. We cannot justify collecting stuff on the odd chance that it will be useful in the future. In fact, the OTA workshop suggested that the problem in medical care is that physicians cannot get access to what they need when they need it. Basic records, like immunizations, are buried in a sea of records that are not accessible at the right time.

I also believe that the insider threat to unauthorized disclosure of patient information is the most potent threat to invasion of privacy especially in low wage situations. An awful lot of people in our respective countries with very low salaries have pretty easy access to sensitive personal information. Instead of the hacker stuff we tend to worry about in various systems, we need to worry about the insider threat-the kind of pressures put on individuals to reveal information about persons-and the kind of gossip factor we talked about earlier.

In 1989 I wrote a book called Protecting ***Privacy in Surveillance Societies.*** It is a study of how privacy works in the public sector in a number of countries, including the United States. It takes a rather negative view of the Privacy Act's utility. It is particularly critical of the lack of a data protection board or a privacy protection commission in this country.

Putting Someone In Charge

Somebody must be put in charge. Enforceable legal remedies should not simply mean to go sue somebody, even if that is the great American pastime. It is not a useful, practical way of solving data protection problems. You have got to have an ombudsperson in place, a privacy protection commission, a data protection board, and state or federal medical information practices commissions. Call it what you want, you need somebody who is looking after things.

Privacy issues are very simple and everybody can understand them. But I regret to say as I listen to people talk about personal privacy especially yesterday morning, that I was reminded of the dramatic difference between novice knowledge of the subject and expert knowledge. While I would be pretentious to claim expert knowledge, after 30 or so years working on the subject, you do know something. And in the federal government we need an ongoing source of expertise on all aspects of privacy and data protection, in addition to the currently critical issues of medical and health information. Even at the state level, several states-including Minnesota, Hawaii, and Wisconsin-have set up state information practice boards, often with jurisdiction over both freedom of information and privacy.

Canada, France, and Britain have all done much better than the United States in making privacy and data protection more meaningful. They have made somebody responsible for making the system work by providing expert advice, by pursuing and investigating complaints, and by conducting audits and investigations of compliance with fair information practices. These kinds of officials can be local, site specific, or at the state or federal levels.

I am encouraged, particularly in Canada, by the emergence of patient ombudspersons in specific hospitals who can often handle complaints and reassure people or pursue their concerns.

The Chaotic State of Data Protection

Despite being an academic, I also believe that privacy security, and data protection measures

of the sort we have been talking about for the last day-and-a-half have to be pragmatic, they have to be realistic, they have to incrementally improve the system. There is probably room for a dramatic step forward, given the chaotic state of data protection for medical and health information in both Canada and in the United States.

I will not discuss the European Community's draft directive on data protection of October 1992, which will be issued in its final form in 1993. But it is a considerable driver in this entire privacy area because countries will be unable to move personal information from country to country if the other countries outside the EC do not have equivalent data protection. The situation in both Canada and the United States is woefully inadequate because we do not have any private sector data protection of a meaningful sort, except for the U.S. Fair Credit Reporting Act. The regimes statewide are really quite chaotic. I regret to say that even in the Province of Ontario, which I tend to regard as my own fiefdom, things are not yet perfect.

What is a Good Patient Record?

We must get some consensus on the appropriate content of a good patient record and insure its accuracy and accessibility It astonishes me, reading the 1991 report on computer-based patient records of the Institute of Medicine, that no agreement has been reached even on what should be in a medical record-never mind who should have access to it.

Secondly, we must ensure informed consent from patients. I do not share Michael Yesley's pessimism about informed consent. A new law, introduced in Quebec in December as a bill to regulate the private sector, is the first of its kind in North America. It specifically provides that an individual cannot be denied a service for refusing to provide certain personal information that is not pertinent to the contract or its execution. You can demand information in order to get a certain service, but if the information is deemed irrelevant to the transaction, you cannot force people to disclose it. And Quebec, typically, has an ombudsperson and a commission that would mediate any complaints about forced disclosure of information.

I have been giving advice to an American company running a huge longitudinal study in Canada about the informed consent form for welfare mothers who are going to be monitored through a period of their lives for both research and administrative purposes. The informed consent form runs four printed pages. I do not like its length and the interviewers do not like it. But it is working in practice, and these people need to know what they are getting themselves in for when they agree to participate in this project.

Making Informed Consent Meaningful

So informational self-determination, that great German principle, can be ensured by making informed consent meaningful. In my vision of the world, somebody. who checks into a hospital ought to be told in considerable detail, unless they are brought in dying or to an emergency room, exactly what is going to be done with their personal information. And if they do not die and if they are going to get a fund raising letter within two months, I want them to be told that in advance. And that is the kind of thing that people should have the right to opt out of. And, in fact, in an ideal informed consent environment, I would even contemplate people saying they would not allow their information to be used for research purposes or some of the other secondary things for which patient information gets used, as much as I am a big fan of that kind of research.

A detailed regime for data disclosures must be developed; Everybody always acts as if that is the most complicated thing in the world. I am holding Bill 50 from British Columbia, enacted in June 1992, which is the best data protection act for the public sector and for freedom of information in existence at the moment. It was enacted in June 1992. Sections 33 to 35 of this bill spell out disclosures of personal information, when a public body may disclose personal information. It goes on for two-and-a-half pages. That kind of regime is in the great American tradition of legislating, and it can be easily adopted. There are no great secrets here. The Germans, the French, the Swedes, the British have been regulating medical information this way for a long, long time.

It is important to think of extending responsibility under data protection regimes by contract, especially when you are dealing with third parties, contractors and customers. That is an important simple notion, well established in American law. You can have written agreements *on* data use that establish what a company will have access to in its medical agreement with Aetna or' whomever. This kind of contractual obligation can really extend the utility of a data protection regime, especially if monitoring, sanctions, auditing, and liability standards are built in.

Developing Fair Information Codes

The development of codes of fair information practices by individual companies is a very important form of self-regulation in which hospitals and physicians' offices and insurance companies can engage. Every doctor's office or hospital should have available a code of fair information practices-in American lingo, privacy codes-so people have some idea of what is going to be done with their personal information. American Express does it, Equifax does it, Canadian banks do it, the telephone companies in Canada do it. Why can the standard hospital or physician's office not establish current practices, without the law telling them what to do? That type of self-regulation can build up from the bottom, can encapsulate and record actual meaningful, established practices-as long as they are good practices. And I expect them to be good practices. This self-regulation coming from the bottom can meet the law coming from the top. It can actually allow the self-regulated to have much more influence on the shaping of statutory regimes, when and if they are enacted, which I obviously hope will be soon.

In the best of all possible worlds, I would like to redo Alan Westin's 1976 empirical study. But I suspect that time may not permit this in the current mood of promoting reformed federal health care.

Regimes for file segregation and file purging are important. More anonymity of data should take place at a certain point, particularly in research files as well as more encryption of stored data. It would be very nice to tell patients in an automated record-keeping system that "your data are encrypted when they are stored, and they are decrypted when someone wants to use them." It sounds good. It actually provides technical protections for the data.

We also need some encouragement to reduce record-keeping that turns hospitals into record-keeping mausoleums.

Sanctions and Civil Liability

Just having pious platitudes on the wall is not enough. You need a way to enforce these rights. Employees must be informed and continuously reminded that they are subject to discipline, including dismissal, for breaches of confidentiality, whether in the record-keeping section or any other part of a hospital or doctor's office. Regimes of civil liability are well established in this country, given the facility and enthusiasm with which people sue one another, but they are also useful.

Most of these kinds of problems handled by a data protection board or a privacy protection commission would find systemic solutions to the problems, rather than having individuals attempt to solve their own problems by suing somebody. I also want to say-and this is perhaps not the most appropriate second to last point-I do not have any difficulties with unique personal identifiers being developed for health identification purposes. I would prefer that, because of the symbolic resistance to it, the social security number not be used. These numbers must be put under very strict controls. Ontario introduced cradle-to-grave or womb-to-tomb numbers-nine digit, unique personal identification numbers-within the last few years. A law was passed to go along with it-the Ontario Health Card Identity Number Act-allowing you to only use these numbers for health-related purposes. A company that collects one number unlawfully is fined $25,000; the fines are $1,000 to $5,000 for individuals who unlawfully collect the numbers. Use of the number for health-related research is permitted. But that number is going to be used, if I have anything to do with it, only for health-related purposes. This is the way it should be done.

Avoiding National Databases

Finally, I am also extremely unhappy when people start talking about a national database. First of all, I think it is unlikely to work; it would be full of problems and even more errors than any other kind of national database, such as the credit reporting file. I think that national databases in the health care field should be avoided like the plague. This is similar to the great national data bank debate of 1965, '66, '67, which some of us are old enough to remember.

Even regional databases, while they may be necessary in areas like New England or the Central Atlantic states, pose various kinds of problems. That may be the obvious level at which databases are to be created. But the more centralization of data, the more risks to breach of privacy and disclosure of personal information that should be kept confidential. ◆◆

APPENDIX A

Task Force

Updated HHS Task Force on the Privacy of Private-Sector Health Records

Joan Turek-Brezina, Chairperson
Office of the Assistant Secretary for Planning and Evaluation

Lois Alexander
Social Security Administration
(through May 1993)

A. Prentice Barnes
Office of the Assistant Secretary for Management and Budget

Johanna Bonnelycke
Office of the Assistant Secretary for Health, PHS

Pat Brooks
Social Security Administration

Susan Callahan
Office of the General Counsel

Thomas Donnelly
Office of the Assistant Secretary for Public Affairs

Willie Etheridge
Administration for Children, Youth, and Families

John P. Fanning
Office of Health Planning and Evaluation, PHS

Richard Friedman
Office of the General Counsel

Herb Hammond
Office of the Assistant Secretary for Planning and Evaluation

Thomas Hoyer
Health Care Financing Administration

W. Keith Lively
Office of the Assistant Secretary for Planning and Evaluation

Stanley Rosenfeld
Health Care Financing Administration
(through June 1993)

Harvey A. Schwartz
Agency for Health Care Policy and Research, PHS

Alan Wilder
Social Security Administration

Patricia Faley, Ex Officio
United States Office of Consumer Affairs

APPENDIX B

Original Task Force Mission Statement

Task Force on the Privacy of Private-Sector Health Records Original Mission Statement

Task Force Mandate

The HHS Task Force on the Privacy of Private-Sector Health Records will examine the extent to which a problem exists regarding use of personally identifiable records by doctors, hospitals, laboratories, pharmacies, insurance companies, medical information bureaus, and other private organizations in the absence of a federal policy to protect individuals from invasions of their privacy, The Task Force also will review current state laws on the privacy of medical records and the status of the recommendations of the Privacy Protection Study Commission of the early 1970s concerning the privacy of these records. The Task Force will consider steps that the federal government could appropriately pursue to protect these nonfederal record systems. Considerations may range from maintaining the status quo to consumer education, proposals for legislation, model state laws, and the strengthening of existing mechanisms for the protection of medical and other health records. At the same, the Task Force must be responsive to legitimate needs for information in the public and private sectors.

In April 1990, Assistant Secretary for Planning and Evaluation Martin H. Gerry established this interdepartmental Task Force.

Task Force members represent the following operating and staff divisions within the department: Administration for Children and Families, Health Care Financing Administration, Public Health Service, Social Security Administration, Office of the Assistant Secretary for Management and Budget, Office of the Assistant Secretary for Planning and Evaluation, Off ice of the Assistant Secretary for Public Affairs, and Office of the General Counsel. Dr. Joan Turek-Brezina, Director, Technical and Computer Support (AWE), serves as chair.

Task Force Activities

To accomplish its mission, the task force has thus far identified the following activities:

- Identify existing private-sector policies and procedures for collecting, using, and disseminating personally identifiable health data as well as policies and procedures that may be adopted in the near future.
  - Identify the types of private-sector organizations that collect, use, and/or disseminate personally identifiable health data (e.g., researchers, direct marketing companies, insurance providers, employers).
  - Identify the type of data being collected, used, and disseminated.
  - Identify the most common methods of data collection.
  - Identify existing policies and procedures for discovering and

correcting inaccurate data resulting from unintentional causes (e.g., mistaken entry negligence) and existing policies and procedures for addressing the consequences of inaccurate data (e.g., Who pays to correct the error?).

- Identify existing policies and procedures for preventing discovering, and correcting intentional misuse of data (e.g., computer security theft, statistical manipulation).
- Analyze reasons personally identifiable health data are being collected, used, and disseminated.
- Identify the principles that govern decisionmaking by private-sector organizations and individuals when determining if an individual's right to privacy should be compromised (e.g., when the health care provider becomes aware that a patient poses a life-threat to another individual).
- Analyze why existing privacy policies and procedures have been adopted and why other policies and procedures have been considered but rejected (e.g., cost, individual's rights considered more important than society's rights).

■ Identify existing privacy problems related to-collect-in-g using and disseminating personally identifiable health data as well as problems that may arise in the near future (e.g., developing trends in computer technology, marketing, or health care record keeping).

- Identify affected populations.
- Identify severity of each problem.
- Identify frequency of occurrence of each problem.
- Identify the facility with which each problem can be corrected.

■ Identify the role ethics, regulation, and legislation have played in the development of existing privacy policies, procedures, and problems as well as the role they could play in establishing future policies and procedures and in preventing future problems.

■ Identify state and local legislation or case law relating to private-sector collection, use, and/or dissemination of personally identifiable health data.

■ Identify existing consumer-education programs that help make the public aware of the ways in which health data are being collected, used, and disseminated and the recourse the public can take if desired.

APPENDIX C

Conference Agenda

HEALTH RECORDS:
SOCIAL NEEDS AND PERSONAL PRIVACY

February 11-12, 1993

Omni Shoreham Hotel, Washington, DC

WEDNESDAY, FEBRUARY 10, 1993		
5:00 - 7:00 P.M.	**Conference Registration**	
THURSDAY, FEBRUARY 11, 1993		
	7:30 A.M. - 5:00 P.M. CONFERENCE REGISTRATION	
8:00 - 9:00 A.M.	**CONTINENTAL BREAKFAST WILL BE SERVED**	
8:30 - 9:00 A.M.	**Welcome**	**Joan Turek-Brezina, Ph.D,** Chairpemon, Task Force on **the** Privacy of Private Sector Heaith Records
	Conference **Overview**	**Gerald Britten, Acting Assistant Secretary for Pianning and Evaluation**
	Opening Remarks	**J. Jarrett Clinton, MD, M.P.H., Administrator, Agency for Health Care Policy and Research**
9:00 - 9:45 A.M.	introduction	**Patricia Faiey, Acting Director of the United States Office of Consumer Affairs**
	Keynote Speech	**Conceptual issues in Maintaining the Balance Between the Privacy of Private Sector Health Records and the Need for information**
	Presentation	**Ruth Faden, Ph.D., Johns Hopkins School of Public Health A discussion of bloethlcai issues**
	9:45 - 4:00 P.M. THE USES OF HEALTH INFORMATION NOW AND IN THE FUTURE: IMPLICATIONS OF AN ELECTRONIC SYSTEM *** A question and** answer period will follow each set of presentations	
9:45 - 11 :00 A.M.	Providers' use of **primary** heaith care data	**Roger Bulger, M.D., Association of Academic Health Centers Peter Waegemann, Medical Records institute**
II:OO- **11:15 A.M.**	BREAK	
11:15 - 12:30 P.M.	**Health** Data and the Private Sector	**Lorna Christie, Direct Marketing Association Stephen Brooks, MA., Aetna Health insurance**
12:30 -1:45 P.M.	LUNCHEON Presentation	**Willis Ware, Ph.D., Privacy Protection Study Commission Lessons for the Future**
1:45 - 3:00 P.M.	Research use of health records: the individuals' contribution to medical knowledge	**David Pryor, M.D., Duke University Medical Center Dale Schumacher, M.D., M.Ed., M.P.H., Rockburn Institute and Commission on Professional and Hospital Activitler**
3:00 - 3:15 P.M.	**BREAK**	
3:15 - 4:00 P.M.	Administrative uses of **health** records: monitoring, government systems, and law enforcement	**Janis Curtis, Y.S.P.H., Duke University Florence M. Rice, Harlem Consumer Education Council**
	4:00 - 5:30 P.M. HOW DOES THE USE OF HEALTH INFORMATION AFFECT INDIVIDUAL RIGHTS?	
4:00 - 5:30 P.M.	Consequences to the individual of data collection and information use, and the development of electronic **health** systems	**Madison Powers, J.D., D. Phil., Kennedy Institute of Ethics, Georgetown University Janlorl Goldman, J.D., American Civil Liberties Union**
5:30 - 7:oo P.M.	RECEPTION	

HEALTH RECORDS:
SOCIAL NEEDS AND PERSONAL PRIVACY
FEBRUARY 11-12, 1993
OMNI SHOREHAM HOTEL, WASHINGTON, DC

FRIDAY, FEBRUARY 12, 1993

8:00 - 9:00 A.M.	CONTINENTAL BREAKFAST WILL BE SERVED	
8:00 - 8:30 A.M.	BREAKFAST ADDRESS	Deirdre Duzor, M.A., Health Care Finance Administration, Department of Health and Human Services The Changing Healthcare Environment
8:30 - 9:15 HOW DOES THE USE OF HEALTH INFORMATION AFFECT INDIVIDUAL RIGHTS (CONTINUED)		
8:30 - 9:15 A.M.	Individual rights and expectations and societal needs	Larry Gostin, J.D., American Society of Law and Medicine and Ethics Michael Yesley, J.D., Los Alamos National Laboratory
9:15 - 10:45 HOW DOES SOCIETY STRIKE THE BALANCE BETWEEN THE PRIVACY OF PRIVATE SECTOR HEALTH RECORDS AND THE NEED FOR INFORMATION?		
9:15 - 10:30 A.M.	Approaches to privacy protection: policies and guidelines	Alan Westin, LL.B., Ph.D., Columbia University Pam Wear, MBA, RRA, American Health Information Management Association John Fanning, LL.B., Public Health Service, Department of Health and Human Services Robert Gellman, J.D., Subcommittee on Government Information, Justice, and Agriculture
10:30 - 10:45 AM.	BREAK	
10:45 - 11:30 A.M.	Ownership, uses, and dissemination of health care information: who is in control?	Vincent Brannigan, J.D., University of Maryland J. Michael Fitzmaurice, Ph.D., Agency for Health Care Policy and Research
11:30 - 12:15 A.M.	CLOSING REMARKS and SYNOPSIS	David Flaherty, Ph.D., University of Western Ontario
12:15 - 12:30 P.M.	ADJOURNMENT	Joan Turek-Brezina, Ph.D., Chairperson, Task Force on the Privacy of Private Sector Health Records

APPENDIX D

Conference Participants

HEALTH RECORDS: SOCIAL NEEDS AND PERSONAL PRIVACY

SPONSORED BY THE TASK FORCE ON PRIVACY, DEPARTMENT OF HEALTH AND HUMAN SERVICES

FEBRUARY 11-12, 1993
OMNI SHOREHAM HOTEL
WASHINGTON, DC

PARTICIPANT LIST

Lois Alexander
Special Assistant Disclosure
Social Security Administration
Department of Health and Human Services
Room 639H, HHH Building
200 Independence Avenue, SW
Washington, DC 20201

Sheri Alpert
Senior Program Analyst
Internal Revenue Service
U.S. Treasury
ISM:S:R:P
1111 Constitution Avenue, NW
Washington, DC 20224

Roxanne Andrews, Ph.D.
Data Development Coordinator
Agency for Health Care Policy and Research
Department of Health and Human Services
Division of Provider Studies
2101 East Jefferson Street, Suite 500
Rockville, MD 20852

John T. Ashley, M.D., M.B.A.
Associate Vice President
University of Virginia
Health Sciences Center, Box 236
Charlottesville, VA 22908

Harvey A. Ashman
Assistant General Counsel
IMS International
100 Campus Road
Totowa, NJ 07512

Donna L. Bacon
Vice President
General Counsel
Medstat Systems, Inc.
777 East Eisenhower Parkway
Ann Arbor, MI 48108

Walter P. Bailey, M.P.H.
Chief, Health and Demographic Statistics
South Carolina State Budget and Control Board
Division of Research and Statistical Services
Rembert C. Dennis Building
Suite 425
1000 Assembly Street
Columbia, SC 29201-3117

John A. Baker
Senior Vice President
Equifax, Inc.
1600 Peachtree Street, NW
Atlanta, GA 30309

A Prentice Barnes
Records Management Officer
Office of the Assistant Secretary
for Management and Budget
Department of Health and Human Services
Room 531H
HHH Building
200 Independence Avenue, SW
Washington, DC 20201

Gilbert W. Beebe, Ph.D.
Health Statistician
National Cancer Institute
National Institutes of Health
6130 Executive Boulevard
EPN 400
Rockville, MD 20895

Aimee R Berenson, J.D.
Legislative Counsel
AIDS Action Council
1875 Connecticut Avenue, NW
Suite 700
Washington, DC 20009

Ron Bernier
President
Physician Computer Network, Inc.
Atrium One
100 Metro Park South
Laurence Harbor, NJ 08878

Rachel H. Bishop, J.D.
Staff Attorney
Office of the General Counsel
U.S. Department of Agriculture
14th & Independence Avenue, SW
Washington, DC 20250-1400

Colonel Gordon C. Black, M.H.A. (Ret.)
Ohio State University
Department of Preventative Medicine
M213 S-L Hall
320 West Tenth Avenue
Columbus, OH 43210

Beverly Boguer, R.R.A.
Program Consultant
Public Health Service
Department of Health and Human Services
Parklawn Building, Room #11-11
5600 Fishers Lane
Rockville, MD 20857

Johanna Bonnelycke
Privacy Officer
Office of the Assistant Secretary for Health
Department of Health and Human Services
Room 17-41, Parklawn Building
5600 Fishers Lane
Rockville, MD 20857

Vincent M. Brannigan, J.D.
Professor of Consumer Law
University of Maryland
College Park, MD 20742

Gerald Britten
Acting Assistant Secretary for Program Systems
Office of the Assistant Secretary
for Planning and Evaluation
Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Stephen Brooks, M.A.
Manager
Medical Information Management
AETNA Health Plans
151 Farmington Avenue (MP34)
Hartford, CT 06156

Jennie L Bryan, R.R.A.
YPRO
2917 Six Mile Lane
Louisville, KY 40220

Roger J. Bulger, M.D.
President
Association of Academic Health Centers
1400 16th Street, NW
Suite 410
Washington, DC 20036

Deborah Burris
Management Analyst
Office of Information Resources Management
Department of Health and Human Services
HHH Building, 531H
200 Independence Ave, SW
Washington, DC 20201

Christopher G. Caine
Manager
Human Resource and Environmental Policy
IBM Corporation
1301 K Street, NW
Washington, DC 20005-3307

Susan Callahan
Office of the General Counsel
Department of Health and Human Services
Room 5541, Cohen Building
330 Independence Avenue, SW
Washington, DC 20201

Jean Cantrell
Director
State Government and Industry Affairs
The Dun and Bradstreet Corporation
1001 G Street, NW #300 E
Washington, DC 20001

Marcia Carlyn, Ph.D.
Director, Research and Evaluation
Prospect Associates
1801 Rockville Pike, #500
Rockville, MD 20853

Lorna Christie
Senior Vice President
Direct Marketing Association
1101 17th Street, NW
Washington, DC 20036-4704

Daniel M. Christy, M.P.A.
Project Manager, RWJ
West Virginia Health Care Planning Commission
405 Capitol Street, Suite 308
Charleston, WV 25301

Robert F. Clark, D.P.A.
Program Analyst
Office of the Assistant Secretary
for Planning and Evaluation
Department of Health and Human Services
Room 424-E, HHH Building, 200
Washington, DC 20201

J. Jarrett Clinton, M.D., M.P.H.
Administrator
Agency for Health Care Planning and Research
Department of Health and Human Services
2101 East Jefferson Street
Suite 600
Rockville, MD 20852

Sarah Comley, Ph.D.
President
International Observers and
North American Biolegal Information
1325 15th Street, NW, #615
Washington, DC 20005

Ann Cooley
National Institutes for Mental Health
Parklawn Building
5600 Fishers Lane
Rockville, MD 20854

John W. Coombs
Director General
Statistics Canada
Canadian Centre for Health Information
20-0X-I Coats Building
Tunney's Pasture
Ottawa, Canada K1A 0T6

Nancy B. Cummings, M.D.
Associate Director, Research and Assessment
National Institute for Diabetes
and Digestive and Kidney Disorders
National Institutes of Health
Room 627
5333 Westbard Avenue
Bethesda, MD 20892

Anne O. Curtis, RRA.
Resource Analyst
National HealthCorp
PO Box 1398
Murfreesboro, TN 37133

Janis L. Curtis, M.S.P.H.
Director
Special Services
Duke University Medical Center
PO Box 3708
Durham, NC 27710

Kimberly Dane
Survey Statistician
U.S. Department of Commerce
Bureau of the Census
Washington, DC 20233-001

Simon Davies
Director
Privacy International
666 Pennsylvania Avenue, SE
Suite 303
Washington, DC 20003

Virginia A. de Wolf, Ph.D.
Mathematical Statistician
U.S. Bureau of Labor Statistics
1719 Luzeme Avenue
Silver Spring, MD 20910

William F. Decker, M.P.A.
Senior Analyst
Health Team, Public Policy Institute
American Association of Retired Persons
601 E Street NW
Washington, DC 20049

Molla Donaldson, M.S.
Senior Staff Officer
Institute of Medicine
National Academy of Sciences
2101 Constitution Avenue, NW
Washington, DC 20418

Thomas E. Donnelly
Privacy Act Officer
Office of the Assistant Secretary
for Public Affairs
Department of Health and Human Services
Room 645F, HHH Building
200 Independence Avenue, SW
Washington, DC 20201

David Duncan
Manager, Research and Systems
Information and Privacy Commission
80 Bloor Street, W
Suite, 1700
Toronto, Ontario
Canada M5S 2V1

Deirdre Duzor, M.A.
Director
Division of Medicare, Part A Analysis
Office of Legislation and Policy
Health Care Financing Administration
Department of Health and Human Services
HHH Building
200 Independence Avenue, SW
Washington, DC 20201

Willie Etheridge
Administration for Children, Youth, and Families
Department of Health and Human Services
Aerospace Building
7th Floor
370 L'Enfant Promenade, SW
Washington, DC 20447

Ruth Faden, Ph.D.
Johns Hopkins School of Public Health
624 North Broadway
Hampton House, Room 509
Baltimore, MD 21205

Patricia Faley
Acting Director
U.S. Office of Consumer Affairs
1620 L Street, NW Suite 700
Washington, DC 20036

John P. Fanning, L.L.B.
Office of Health Planning and Evaluation
Department of Health and Human Services
Room 740G, HHH Building
200 Independence Avenue, SW
Washington, DC 20201

J. Michael Fitzmaurice, Ph.D.
Director
Office of Science and Data Development
Agency for Health Care Policy and Research
Department of Health and Human Services
2101 E. Jefferson, Suite 604
Rockville, MD 20852

David H. Flaherty, Ph.D.
Professor of History and Law
University of Western Ontario
London, Ontario
Canada

Teresea Foley, R.R.A., M.A.
Medical Record Consultant
Office of the Army Surgeon General
5109 Leesburg Pike
Falls Church, VA 22041-3258

A.M. Frager
Vice President
Information Spectrum Inc.
5107 Leesburg Pike
Falls Church, VA 22041

Clara L. French
Food Program Specialist
Food and Nutrition Service
U.S. Department of Agriculture
3101 Park Center Drive, Room 540
Alexandria, VA 22302

Richard M. Friedman, J.D.
Office of the General Counsel
Department of Health and Human Services
Room 5362, Cohen Building
330 Independence Avenue, SW
Washington, DC 20201

Diane Fulton
Analyst
Blue Cross and Blue Shield Association
1310 G Street, NW
Washington, DC 20005

Michele A. Gargano, M.Sc.
Research Assistant
Kunitz and Associates, Inc.
6001 Montrose Road
Suite 920
Rockville, MD 20852

Margaret Garikes, J.D.
Assistant Director for Federal Affairs
American Medical Association
1101 Vermont Avenue, NW
Washington, DC 20005

Gerald W. Gates
Administration Records Program Officer
Bureau of the Census
U.S. Department of Commerce
Washington, DC 20233-001

Robert Graubart
MITRE Corporation
202 Burlington Road
MS B330
Bedford, MA 01730

Robert Gellman, J.D.
Chief Counsel
Subcommittee on Government Information, Justice, and Agriculture
B349C Rayburn
U.S. House of Representatives
Washington, DC 20515-6147

Beth Givens
Project Director
Privacy Rights Clearinghouse
Center for Public Interest Law
University of San Diego
5998 Alcala Park
San Diego, CA 92110-2492

Janlori Goldman, J.D.
Legislative Council
American Civil Liberties Union
Privacy and Technology Project
122 Maryland Avenue, NE
Washington, DC 20002

Eric Gorovitz
Georgetown University School of Law and
Johns Hopkins School of Public Health
149 Dunnington Place, SE
Washington, DC 20003

Larry Gostin, J.D.
American Society of Law
and Medicine and Ethics
765 Commonwealth Avenue
Boston, MA 02215

Greg Gould
Legal Counsel
Montana Cooperative Center
for Health Information
P.O. Box 4210
Helena, Montana 59620

Elizabeth B. Gravatte, M.B.A.
Government Affairs Manager
Hewlett-Packard Company
900 17th Street, NW, Suite 1100
Washington, DC 20006

Marjorie S. Greenberg, M.A.
Evaluation Officer
National Center for Health Statistics
Centers for Disease Control
6525 Belcrest Road
Room 1100
Hyattsville, MD 20782

Albert L. Haggard, J.D., RN.
Director of Risk Management
Scott & White Hospital & Clinic
2401 SO. 31st Street
Temple, TX 76508

Herbert Hammond, M.P.A.
Policy Analyst
Office of Health Policy
Department of Health and Human Services
200 Independence Avenue, SW
Room 442 E
Washington, DC 20201

Malcolm Harriman, M.A.
President
HealthExpert Systems, Inc.
7600 66 Street N.
Pinellas Park, FL 34665

Ruth Heltzer
Research Administrator
Kunitz and Associates, Inc.
6001 Montrose Road
Suite 920
Rockville, MD 20852

Evan Hendricks
Editor and Publisher
Privacy Times
P.O. Box 21501
Washington, DC 20009

Beth Herse
Staff Counsel
Office of Statewide Health
Planning and Development
1600 9th Street, Room 435
Sacramento, CA 95814

Timothy Hill
Presidential Management Intern
200 Independence Avenue, SW
Room 341-H-HHH Building
Washington, DC 20201

James Hudson, M.D.
Professor of Epidemiology
and Preventative Medicine
University of Maryland
School of Medicine
655 W Baltimore Street
Baltimore, MD 21201

Shirley Hughes
Director of Advanced Technology
EMTEK Health Care Systems
1501 W. Fountainhead Parkway, Suite 190
Tempe, AZ 85282

Pat Ivie, A.RT.
Medical Record Consultant
National HealthCorp, L.P.
P.O. Box 767
Lawrenceburg, TN 38464

Chauncey B. Jessup, M.A.
Archivist
National Archives
NSXA- Center for Electronic Records
Room 20-E
Washington, DC 20408

Ronald S. Jolda, D.O.
CEO
Professional Data Management Group
P.O.Box 3581
North Anson, ME 04958

Marvin S. Kalachman, M.H.A.
Clinical Administrator
Bradley Hospital
1011 Veterans Memorial Parkway
East Providence, RI 02915

Caren Kamberg, M.S.P.H.
Research Administrator
The RAND Corporation
2100 M Street, NW
Washington, DC 20037-1270

Frank L. Kirby
Director, Data Release Policy Staff
Health Care Financing Administration
Department of Health and Human Services
Room 3A12 - SOP Building
6325 Security Blvd
Baltimore, MD 21207

Rene C. Kozloff, Ph.D.
Vice President
Kunitz and Associates, Inc.
6001 Montrose Road
Suite 920
Rockville, MD 20852

Selma C. Kunitz, Ph.D.
President
Kunitz and Associates
6001 Montrose Road
Suite 920
Rockville, MD 20852

Barbara Kurtzig
Associate Director
National Association of
Health Data Organizations
254-B North Washington Street
Falls Church, VA 22046-4517

Alana Landey, M.P.A.
Program Analyst
Food and Nutrition Service
U.S. Department of Agriculture
3101 Park Center Drive, Room 212
Alexandria, VA 22302

Larry M. Lawrence, M.A., M.B.A.
Group Leader
The MITRE Corporation
7125 Colshire Drive
McLean, VA 22102-3481

Ted Leventhal
Contributing Editor
Privacy Times
P.O. Box 21501
Washington, DC 20009

Helen G. Levy
Mathematician
Agency for Health Care Policy and Research
Department of Health and Human Services
2101 East Jefferson Street, Suite 600
Rockville, MD 20852

Cathy Lewis
Staff Assistant
Senate Governmental Affairs Committee
U.S. Senate
340 Dirksen
Washington, DC 20510

Maureen Y. Lichtveld, M.D., M.P.H.
Assistant Director for Public Health Practice
Agency for Toxic Substances & Disease Registry
Centers for Disease Control
1600 Clifton Road, MS-E32
Atlanta, GA 30333

W. Keith Lively
Deputy to the Deputy Assistant Secretary
for Program Systems
Office of the Assistant Secretary
for Planning and Evaluation
Room 447D, HHH Building
200 Independence Avenue, SW
Washington, DC 20201

Kathleen N. Lohr, Ph.D.
Deputy Director,
Division of Health Care Services,
Institute of Medicine
National Academy of Sciences
2101 Constitution Avenue, NW
Washington, DC 20418

Julian Manelli, M.A.
Deputy Director
Division of Disability Processing Policy
Social Security Administration
Department of Health and Human Services
6401 Security Boulevard
3 A-10 Operations
Baltimore, MD 21205

Mary Moien, M.S.
Assistant to the Director
National Center for Health Statistics
Centers for Disease Control
6525 Belcrest Road, Room 1140
Hyattsville, MD 20782

Brenda Monroe
Senior Consultant
Price Waterhouse
1801 K Street, NW
Suite 700
Washington, DC 20006

Edwin Morgan
Manager
Medical Systems
Aspen Systems Corporation
962 Wayne Avenue
Suite 701
Silver Spring, MD 20910

John Norris, J.D., M.B.A.
Corporate Executive Vice President
Hill and Knowlton
800 South Street
Waltham, MA 02154

Meg O'Donnell
Counsel
Health Care Authority
89 Main Street, Drawer 20
Montpelier, VT 05620-3601

Stan Phillips
Agency for Health Care Policy and Research
Department of Health and Human Services
2101 East Jefferson Street, Suite 604
Rockville, MD 20852

Cindy Pierson
Consultant
Naval Medical Information Management Center
1119 Agnew Drive
Rockville, MD 20851

Madison Powers, J.D., D.Phil.
Senior Research Scholar
Kennedy Institute of Ethics
Georgetown University
1437 37th Street, NW, Room 209
Washington, DC 20057

Thomas E. Price, Ph.D.
Privacy Officer
Social Security Administration
Department of Health and Human Services
6401 Security Boulevard
Baltimore, MD 21235

David Pryor, M.D.
Associate Professor of Medicine
Duke University Medical Center
PO Box 3531
Durham, NC 27710

David M. Radosevich, Ph.D., M.S.P.H.
Senior Research Scientist
Health Outcomes Institute
2001 Killebrew Drive
Suite 122
Bloomington, MN 55425

John C. Rahiya
Vice President
Equifax, Inc.
1600 Peachtree Street, NW
Atlanta, GA 30309

Virginia Randall, M.D.
Consultant to the Surgeon General
Office of the Army Surgeon General
3804 Cherry Valley Drive
Olney, MD 20832

Florence M. Rice
Harlem Consumer Education Council
Triboro Station
P.O. Box 1165
New York, NY 10035

Stanley Rosenfeld
Health Care Financing Administration
Department of Health and Human Services
Room 433, EHR Building
6325 Security Boulevard
Baltimore, MD 21207

Gwen Rubinstein, M.P.H.
Health Policy Analyst
Office of the Assistant Secretary
for Planning and Evaluation
Department of Health and Human Services
200 Independence Ave, SW, Room 442-E
Washington, DC 20201

Kathy H. Rufo, M.P.H.
Assistant Director for Management
Division of Epiemiology and Surveillance
1600 Clifton Road (C08)
Centers for Disease Control and Prevention
Atlanta, GA 30333

Julia L Sameth
Research Assistant
Kunitz and Associates, Inc.
6001 Montrose Road
Suite 920
Rockville, MD 20852

Dale Schumacher, M.D., M.Ed., M.P.H.
President, Rockburn Institute and
Senior Medical Advisor,
Commission on Professional
and Hospital Activities
1105 Eisenhower Place
PO Box 304
Ann Arbor, MI 48106

Harvey A. Schwartz, Ph.D.
Senior Economist
Agency for Health Care Policy & Research
Department of Health and Human Services
2101 East Jefferson Street, Suite 604
Rockville, MD 20852

Jerome Seidenfeld, Ph.D.
Senior Scientist
American Medical Association
515 N. State Street
Chicago, IL 60610

Richard S. Sharpe
Program Director
The John A. Hartford Foundation
55 East 59th Street
New York, NY 10022

Robert Ellis Smith
Publisher
Privacy Journal
P.O.Box 28577
Providence, RI 02908

Deborah Stone, M.Ed.
Research Psychologist
U.S. Bureau of Labor Statistics
Behavioral Science Research Center
2 Massachusetts Avenue, NE
Mail Stop 4915
Washington, DC 20212-0001

Sharon L Stumbo, M.A., M.H.A.
Deputy Commissioner
Cabinet for Human Resources
Kentucky Department for Health Services
275 East Main Street
Frankfort, KY

Phillip A. Surine
Program Analyst
Health Care Financing Administration
Department of Health and Human Services
2-D-2 ME Building 6325 Security Boulevard
Baltimore, MD 21224

Randy L Teach
Washington Representative
Medical Group Management Association
1156 15th Street, NW, Suite 1100
Washington, DC 20005

Karen Smith Thiel, Ph.D.
Director
Healthy Start Evaluation
Health Resources and Services Administration
Department of Health and Human Services
Parklawn Building, Room 14-36
5600 Fishers Lane
Rockville, MD 20857

Joan Turek-Brezina, Ph.D.
Chair, Task Force on Privacy
Office of the Assistant Secretary
for Planning and Evaluation
Department of Health and Human Services
200 Independence Avenue, SW
Room 438F HI-II-I Building
Washington, DC 20201

Pat Urban
Data Administrator
Health Care Authority
89 Main Street, Drawer 20
Montpelier, VT 05620-3601

Marie van Mel&Wright, Ph.D.
Senior Research Psychologist
U.S. Bureau of Labor Statistics
Behavioral Science Research Center
2 Massachusetts Avenue, NE,
Mail Stop 4915
Washington, DC 20212-0001

Pat Venus
Manager
Research Services
United HealthCare Corporation
9900 Bren Road East
P.O. Box 1459
Minneapolis, MN 55440-8001

Peter Waegemann
Executive Director
Medical Records Institute
PO Box 289
Newton, MA 02160

Derek Wang, Ph.D.
Executive Assistant
Social Security Administration
Department of Health and Human Services
ALT 250
6401 Security Boulevard
Baltimore, MD 21235

Willis H. Ware, Ph.D.
Corporate Research Staff
The RAND Corporation
1700 Main Street
Santa Monica, CA 90407

Linda K. Watson
Supervisory Program Analyst
Health Care Financing Administration
Department of Health and Human Services
2-D-2 ME Building 6325 Security Boulevard
Baltimore, MD 21224

Pam Wear, M.B.A., R.R.A.
Executive Director
American Health Information
Management Association
919 North Michigan Avenue, Suite 1400
Chicago, IL 60611-1683

Dorothy Webman, M.S.W.
Senior Associate for Program Development
Albert E. Trieschman Center
1968 Central Avenue
Needham, MA 02192

Alan F. Westin, Ph.D.
Columbia University
1100 Trafalgar Street
Teaneck, NJ 07666

Janet Wise
Program Analyst
Data Release Policy Staff
Health Care Financing Administration
Department of Health and Human Services
6325 Security Boulevard
Baltimore, MD 21207

Rose L. Woodburn
Internal Revenue Service
U.S. Treasury
Statistics of Income Division
R:S:P
1111 Constitution Avenue, NW
Washington, DC 20224

Michael Yanoff
Chief, Privacy Staff
Internal Revenue Service
U.S. Treasury
ISM:S:R:P
1111 Constitution Avenue, NW
Washington, DC 20224

Michael Yesley, Ph.D.
Los Alamos National Lab
MS Al87
Los Alamos, NM 87545

Wendy L. Zahler, J.D.
Attorney
Benesch, Friedlander, Coplan & Aronoff
1100 Citizens Building
850 Euclid Avenue
Cleveland, OH 44114

APPENDIX E

Conference Synopsis

HEALTH RECORDS: SOCIAL NEEDS AND PERSONAL PRIVACY

SPONSORED BY THE TASK FORCE ON PRIVACY,
DEPARTMENT OF HEALTH AND HUMAN SERVICES

FEBRUARY 11-12, 1993
OMNI **SHOREHAM HOTEL**
WASHINGTON, DC

CONFERENCE SYNOPSIS

CONFERENCE WELCOME

Thursday, February 11, 1993 from 8:30 - 8:45 A.M.

Joan Turek-Brezina, Ph.D.
Chair, Task Force on Privacy
Office of the Assistant Secretary for Planning and Evaluation

CONFERENCE OVERVIEW

Thursday, February 11, 1993 from 8:45 - 9:00 A.M.

Gerald Britten
Acting Assistant Secretary for Program Systems

These remarks will give an overview of the conference and will outline the remaining conference. Included will be a brief overview of privacy issues, the need for data for research, the need to find the balance between the two as well as the implications of an electronic health system.

OPENINGREMARKS

Thursday, February 11, 1993 from 8:45 - 9:00 A.M.

J. Jarrett Clinton, M.D., M.P.H.
Agency for Health Care Policy and Research

These remarks will define the goals and objectives for the conference and establish the overall theme for the presentations. The perspective of the Agency for Health Care Policy and Research on maintaining the balance between the privacy of health records and the legitimate needs for information while facilitating the development of electronic health information systems will be presented.

KEYNOTE ADDRESS
Thursday February 11, 1993 from 9:00-9:45 A.M.

Ruth Faden, Ph.D.
Johns Hopkins University

Maintaining the balance between the privacy of private sector health records and the need for information: an overview

This session will set the stage for the conference by discussing the uses of health information, the effect of health information upon individual rights, and the best means to maintain the balance between the privacy of health records and the need for data in the future as we move towards electronic health information.

PROVIDERS USE OF PRIMARY HEALTHCARE DATA
Thursday, February 11, 1993 from 9:45-11:00 A.M.

This session focuses on the ways in which data collected for routine health care are used for reasons other than those for which they were primarily collected. Use of data by the person(s) who collected them or by others who have been granted access to them, both within the institution and outside of it, will be addressed. Specifically, this session will address:

- Contents of the primary health record and the electronic medical record;
- The implications of large record systems and automation in the collection and use of individual patient data;
- Patient and provider expectations for access to and control of information;
- Providers relationship to other sectors of the health care community in relation to the use of patient data;
- The value of data to the patient and the provider; and
- Costs and benefits of health care data to the provider and the patient.

Roger Bulger, M.D.
Association of Academic Health Centers

- Patients' privacy and confidentiality rights in the emerging world of computer-based, medically relevant information
- Effect of information technology on privacy rights

- The primary health record and the electronic medical record
- Limiting access to data
- Benefits and harms to the patient and provider of Automated Record Systems

Peter Waegemarm
Medical Record Institute

- Requirements in designing confidentiality measures
- Areas where a national consensus must be achieved
  - Potential harm through information misuse
  - Definition of which information can be harmful
  - Methods of information accessing and dissemination that can lead to violations of privacy
  - General understanding of confidentiality measures
  - Practical guidelines for the systems planner and computer systems implementor

HEALTH DATA AND THE PRIVATE SECTOR
Thursday, February 11, 1993 from 11: 15 - 12:30 P.M.

This session focuses on the ways in which private sector organizations, such as health and other types of insurers, direct marketers, credit bureaus, and employers, use data for reasons other than for which they were primarily collected. Use of data by the person(s) who collected them or by others who have been granted access to them, both within the organization and outside of it, will be addressed. Specifically, this session will address:

- Steps that are taken by private sector organizations to produce health related data, reports, and other information;
- Secondary uses of health data in the private sector;
- Use of health care records that affect the individual directly versus use of health care records not intended to affect individuals directly;
- The value of data to the individual and to the private sector.

Lorna Christie
Direct Marketing Association

The Use of Personal **Health** Data for Marketing Purposes

- Direct Marketing

- Limited use made of health records for marketing purposes
- Potential for abuse
- Means by which health data disclosed in non-health records appears in mailing lists

- Direct Marketing Association @MA)
  - Limiting the use of sensitive data for marketing purposes
  - DMA's link to principles contained in the 1973 HEW Advisory panel report on privacy
  - DMA's program as a model for privacy programs

- How consumers can protect their privacy

Stephen P. Brooks, M.A.
Aetna Health Insurance

- Introduction: health data and the private sector - a unique privacy issue?
- Healthcare and information technology trends
- Private sector health data
- Traditional uses of health data in the private sector
  - Process claims and pay benefits
  - Customer Service
  - Financial and actuarial analysis
- Other uses of health data in the private sector
  - Develop and manage provider networks
  - Product design
  - Pharmacy drug interactions and patient profiles
  - Visit reminders, prescription refill reminders
  - Targeted health education programs
  - Patient risk assessments
  - Detect and pursue fraud

- Uses for non-medical/non-benefits related purposes
- Does the use of health care data by the private sector present a unique privacy issue?
- Where do we go?

LUNCHEON ADDRESS
Thursday February 11, 1993 from 12:30-1:45 P.M, during the luncheon

Willis Ware, Ph.D.
The RAND Corporation

Privacy Protection Study Commission: Lessons for the Future

This luncheon address will focus on the findings of the Privacy Protection Study Commission as they relate to the development of the electronic health system and health records. Proposed changes in the health care delivery system such as electronic processing of insurance claims and payments, the automation of health care records, arid the use of a unique patient identifier have implications for patient privacy and confidentiality that have been addressed in earlier work on privacy protection.

RESEARCH USES OF HEALTH RECORDS: THE INDIVIDUAL AS CONTRIBUTOR TO MEDICAL KNOWLEDGE
Thursday February 11, 1993 from 1:45-3:00 P.M.

This session will focus on the ways in which data collected for routine health care are used by researchers to achieve important findings that benefit the individual and society at large while safeguarding the confidentiality of the patient. The speakers will also address the use of data by the person(s) who collected them and the access to and use of data by person(s) other than the original collector.

David Pryor, M.D.
Duke University

- The public and private good created by researchers' access to patient's health care information;
- The benefits of electronic patient care information and how it contributes to useful research findings; and
- Research in the private and the public sector.

Dale N. Schumacher, M.D., M.Ed., M.P.H.
Rockburn Institute
Commission on Professional and Hospital Activities

- The positions of private sector researchers and sponsors;
- The benefits and dangers of using linked medical files with data about individual patients, as well as masking and mixing data; and

- Governing information alliance and privacy and healthcare reform; specifically inputs, process, and outcomes.

ADMINISTRATIVE USES OF HEALTH RECORDS: MONITORING, GOVERNMENT SYSTEMS, AND LAW ENFORCEMENT
Thursday February 11, 1993 from 3: 15 - 4:00 P.M.

This session will focus on:

- The use of automated health records by the government for audit, monitoring, and public health surveillance;

- The detection of fraud and abuse in the management of claims and reimbursement in the private and public sector;

- The use of private sector health records in law enforcement

Issues to be considered are the implications of how these data are used on the privacy and confidentiality rights of the patient.

Janice Curtis, M.S.P.H.
Duke University

- Uses by state agencies of the health data collected by State Data Commission
- Need to recognize uses of health data
  - different agencies
  - different areas of responsibility
  - unique information needs related to decision making
- Uses for hospital charge and utilization data and for public health data
  - mechanisms in place to protect patient confidentiality
  - distinguishing patient level data from patient identifying data
- Challenges faced by state agencies as demands for health data grow

Florence M. Rice
Harlem Consumer Education Council

Automation Denial of Opportunity which Denies the Minority Community the Right to Privacy.

- The use of automated health records by the government for auditing, monitoring, and public health surveillance; and

- The use of private se&or health records in law enforcement.

CONSEQUENCES TO THE INDIVIDUAL OF DATA COLLECTION AND INFORMATION USE and **INDIVIDUAL RIGHTS AND EXPECTATIONS AND SOCIETAL NEEDS**

Thursday, February 11, 1993 from 4:00 - 5:30 P.M.

During this session the speakers will focus on the ways in which the use of health information affects individual rights, the consequences of data collection to the individual, and individual expectations and social needs or privacy rights and protections.

Madison Powers, J.D., D.Phil.
Kennedy Institute of Ethics

- Secondary uses of data and risks to the individual as a result of third party reimbursement, law enforcement and litigation, epidemiological research and other business purposes;
- Consent, its voluntariness, and disclosure of information from the perspective of the patient and the provider; and
- Access to information by the patient and caregiver, access to information for research and budget priorities, and classification of information on the basis of privacy concerns.

Janlori Goldman, J.D.
American Civil Liberties Union

- The absence of legislation designed to protect individual medical and insurance records and the potential for privacy intrusions resulting from computerization of health information;
- Possible limitations on the collection and disclosure of personal health records held by others and security measures for computerized health networks;
- The lessons that have been learned from medical records with special sensitivity such as AIDS, psychiatric, and dependency records, as well as genetic testing; and
- The creation of an individual's "right of access" to personal information.

BREAKFAST ADDRESS
THE CHANGING HEALTHCARE ENVIRONMENT
Friday February 12, 1993 from 8:00-8:30 A.M.

The session will focus on the changes that are taking place in health care delivery and

reimbursement and the impact that an electronic health information system will have in the emerging environment. Issues to be considered are the effects of proposed changes such as the electronic processing of insurance claims and payments, the automation of health care records, and the use of a unique patient identifier on patient privacy and confidentiality.

Dierdre Duzor, M.A.
Office of Legislation and Policy
Health Care! Finance Administration

- Introduction - The Role of Information in Health Care Reform and Beyond
- What and Why Information is critical to health care reform
- Where we are in the process of developing and implementing information systems
- Role of Federal Legislation
- Computerized Clinical Information - Vision of the Future

CONSEQUENCES TO THE INDIVIDUAL OF DATA COLLECTION AND INFORMATION USE and **INDIVIDUAL RIGHTS AND EXPECTATIONS AND SOCIETAL NEEDS**

Friday, February 12, 1993 from 8:30 - 9:15 A.M.

During this session the speakers will focus on the ways in which the use of health information affects individual rights, the consequences of data collection to the individual, and individual expectations and social needs.

Larry Gostin, J.D.
American **Society of Law and Medicine and Ethics**

- The need to protect the individual and the individual's rights as well as the need to consider the public good;
- The balance between the personal and financial costs of providing and collecting data and the benefits received;
- The lessons that have been learned from medical records with special sensitivity such as AIDS, psychiatric, and dependency records, as well as genetic testing; and
- The stigmatizing effects and other unwitting hazards that are potential dangers for the individual as personal data is collected and used.

Michael Yesley, J.D.
Los Alamos National Laboratory

- The special issues, such as genetic testing, which are related to the use of health records in employment, insurance, and credit which directly affect the individual;

- The rights of the individual, with genetics used as a case study, in relation to unconsented disclosure to outside parties and informed consent; secondary uses of data in research, databanks, and industry, access to personal data; and the right not to know; as well as

- Effective policymaking, special efforts to end genetic discrimination, and the implications of the electronic health record.

APPROACHES TO PRIVACY PROTECTION
Friday February 12, 1993 from 9:15 - 10:30 A.M.

This session focuses on the ways in which society strikes the balance between the privacy and confidentiality of health records and the need for information. The speakers will address the legal structures and privacy protections which currently exist and those that will need to be developed as the nation moves towards electronic health records. The development of measures to regulate electronic data transmission from insurers and private industry will also be considered.

Alan Westin, LL.B., Ph.D.
Columbia University

- The contemporary, computer-supported environment in various zones, such as direct care, payment and review, and social uses; the movement of records between these zones; and the need to find a balance in recent trends;

- Today's problems with notice, consent, and release as meaningful protections as well as the problem of regional and national information flows in a state-based legal framework; and

- The role for organizations and associations in this environment and development of a national health information system and the need for impact-analyses and anticipative standards.

Pam Wear, MBA, RRA
American Health Information Management Association

- Existing limitations on the amount and type of data collected and the legitimate uses of this data including individual access, primary and secondary records, and standards and education;

- Regulation of electronic data transmission from insurers and private industry including reliability of hardware and software, the accuracy of the record-keeping process, and maintenance and recovery procedures; and

- Confidentiality agreements, ongoing security and audit trails, and encryption as protective measures as well as cultural change and ethical responsibility as the nation moves towards electronic medical records.

John P. Fanning, LL.B.
Office of Health Planning and Evaluation

- The legal structures and privacy protections that currently exist and those that will need to be developed;

- Regulation of electronic data transfer, auditing, and standards.

Robert C. Gelhnan, J.D.
Subcommittee on Government Information, Justice, and Agriculture

Comments on the preceding speakers' presentations.

OWNERSHIP, USES, AND DISSEMINATION OF HEALTH CARE IN-FORMATION: WHO IS IN CONTROL?
Friday, February 12, 1993 from 10:45 to 11:30 A.M.

Vincent Brannigan, J.D.
University of Maryland

- Legal concept of medical data privacy
- Conflict between privacy expectations of patients and convenience of hospitals
- Problems created in privacy protection by computer systems
- Addressing problems created by special issues (AIDS)
- The role of Regulatory Effectiveness Analysis in technology regulation and privacy protection

J. Michael Fitzmaurice, Ph.D.
Agency for Health Care Policy and Research

- How society strikes the balance between the privacy and confidentiality of private sector health records and the need for data; and

- Various types of safeguards and technological considerations that must be addressed to understand the implications of data use and management on the privacy and confidentiality rights of the patient.

CLOSING REMARKS

Friday February 12, 1993 from 11:30-12:15 A.M.

David Flaherty, Ph.D.
University of Western Ontario

This session will summarize and synthesize the proceedings of the previous day and a half. Comments will be directed toward the issues involved in developing standards and requirements for privacy and confidentiality protection as we move towards an electronic health information system.