HEALTH PRIVACY PROJECT
Institute for Health Care Research and Policy
Georgetown University

best principles FOR HEALTH PRIVACY

A REPORT OF THE
Health Privacy Working Group

WITH SUPPORT FROM
The Robert Wood Johnson Foundation

THE HEALTH PRIVACY WORKING GROUP

The Health Privacy Working Group is an initiative of the Health Privacy Project of Georgetown University's Institute for Health Care Research and Policy. The Working Group is funded through a generous grant from the Robert Wood Johnson Foundation.

The Working Group is staffed by Janlori Goldman, Director, and Zoe Hudson, Policy Analyst of the Health Privacy Project. The Project wishes to thank the Robert Wood Johnson Foundation, in particular Judith Whang, who recognized the importance of this challenge; the Glen Eagles Foundation and the Trellis Fund, most notably Betsy Frampton and Hope Gleicher, who saw the promise in this Project; Andy Burness, Linda Loranger, and the rest of the staff of Burness Communications for their guidance throughout the process; Scott Sanders of High Noon Communications, Audrey Denson of Denson Design, and Mike Heffner of 202 Design for their keen design skills; and our colleagues at the Institute for Health Care Research and Policy.

Our deep appreciation goes to the individual members of the Working Group, who dedicated themselves over the past year to this extremely daunting—and we hope just as valuable—endeavor. As Chair, Dr. Bernard Lo brought to bear his vast knowledge and talents as doctor, ethicist, teacher, writer, listener and refiner, all of which made this possible.

MEMBERS

HEALTH PRIVACY WORKING GROUP
BEST PRINCIPLES FOR HEALTH PRIVACY

EXECUTIVE SUMMARY

Privacy and confidentiality have long been recognized as essential elements of the doctor-patient relationship. Also essential to optimal care is the compilation of a complete medical record. But that same record is used for a wide variety of purposes—including insurance functions, coordination of care, and research. The long-standing friction between these two goals—patient privacy and access to information for legitimate purposes—has been heightened by the transition to electronic health information and a push toward integrated information in support of integrated health care delivery and health data networks. While these developments are intended to improve health care, they also raise many questions about the role of privacy in the health care environment.

Recent polls demonstrate that the public has significant concern about the lack of privacy protection for their medical records and that it can impact how they engage with health care providers. In order to protect their privacy, some patients lie or withhold information from their providers; pay out-of-pocket for care; see multiple providers to avoid the creation of a consolidated record; or sometimes avoid care altogether. Such "privacy-protective" behavior can compromise both individual care and public health initiatives.

The public has some reason to be concerned. Today, there is little consistency in approaches to patient confidentiality and no national standards or policies on patient confidentiality. The 1996 Health Insurance Portability and Accountability Act provides that if Congress fails to enact comprehensive health privacy legislation by August 1999, the Secretary of Health and Human Services must issue regulations. Therefore, either through legislation, government regulation, or self-regulation, there will be significant developments with regard to health privacy in the next two years.

What has been missing from the debate is a consensus document that offers policy recommendations regarding how best to protect patient confidentiality. To fill this void, the Health Privacy Project, with funding from the Robert Wood Johnson Foundation, created the Health Privacy Working Group in June 1998. Its mission was to achieve common ground on "best principles" for health privacy, while identifying a range of options for putting those principles into practice. The Working Group is comprised of diverse stakeholders, including: disability and mental health advocates; health plans; providers; employers; standards and accreditation representatives; and experts in public health, medical ethics, information systems, and health policy.

The Working Group spent the past year crafting a consensus document that reflects "best principles" for health privacy. This report outlines the 11 principles to which the Working Group agreed and details the rationale behind the recommendations.

The principles represent significant compromises between Working Group members and should be seen as a framework that aims to accommodate the various information needs of diverse interest groups. The principles are designed to establish a baseline of

protections that should be considered when implementing comprehensive patient privacy policies and practices.

The Working Group adopted the following 11 principles. Because these principles are intended to establish a comprehensive framework, they should be read and implemented as a whole.

1. For all uses and disclosures of health information, health care organizations should remove personal identifiers to the fullest extent possible, consistent with maintaining the usefulness of the information.

Generally, the use and disclosure of information that does not identify individuals does not compromise patient confidentiality. As such, the use and disclosure of non-identifiable health information should "fall outside" the scope of policies that govern personally identifiable health information. Health care organizations will need to take into consideration the practicality and cost of using and disclosing non-identifiable information. Ultimately, through the creation and use of non-identifiable health information, more people can have more information, without compromising patient confidentiality.

2. Privacy protections should follow the data.

All recipients of health information should be bound by all the protections and limitations attached to the data at the initial point of collection. Recipients of health information can use or disclose personally identifiable health information only within the limits of existing authorizations. Any further uses or disclosures require specific, voluntary patient authorization.

3. An individual should have the right to access his or her own health information and the right to supplement such information.

All patients should be allowed to copy their records and to supplement them if necessary. But supplementation should not be implied to mean "deletion" or "alteration" of the medical record. Furthermore, data holders may charge a reasonable fee for copying the records, but they cannot refuse inspection of the records simply because they are owed money by the individual requesting inspection.

In certain cases, patients may be denied access to their medical records. Such instances include if the disclosure could endanger the life or physical safety of an individual; if the information identifies a confidential source; if the information was compiled in connection with a fraud or criminal investigation that is not yet complete; or if the information was collected as part of a clinical trial that is not yet complete and the patient was notified in advance about his or her rights to access information.

4. Individuals should be given notice about the use and disclosure of their health information and their rights with regard to that information.

The notice should tell the patient how information will be collected and compiled, how the collecting organization will use or disclose the information, what information the patient can inspect and copy, steps the patient can take to limit access, and any consequences the patient may face by refusing to authorize disclosure of information.

5. Health care organizations should implement security safeguards for the storage, use, and disclosure of health information.

Security safeguards consistent with the Secretary of Health and Human Service's standards, whether technological or administrative, should be developed to protect health information from unauthorized use or disclosure and should be appropriate for use with electronic and paper records. Any safeguards should recognize the trade-off between availability and confidentiality and should be tailored to meet needs as organizations adopt more sophisticated technologies.

6. Personally identifiable health information should not be disclosed without patient authorization, except in limited circumstances. Health care organizations should provide patients with certain choices about the use and disclosure of their health information.

Patient authorization should be obtained prior to disclosure of any health information. But, at the same time, some patient information needs to be shared for treatment, payment, and core business functions. With this in mind, the Working Group recommends a two-tiered approach to patient authorization.

The authorization structure allows for a health care organization to obtain a single, one-time authorization for core activities that are considered necessary or routine. These activities are directly tied to treatment, payment, and necessary business functions in keeping with medical ethics. The health care organization may condition the delivery of care—identified as Tier One—or payment for care upon receiving authorization for these activities, which can be obtained at the point of enrollment or at the time of treatment.

Any activities that fall outside this core group (sometimes commonly referred to as uses) must be authorized separately by the patient and fall under Tier Two authorization. The patient can refuse authorization for these activities without facing any adverse consequences. Activities in this category include, but are not limited to:

- purposes of marketing;
- disclosure of psychotherapy notes;
- disclosure of personally identifiable health information to an employer, except where necessary to provide or pay for care;
- disclosure of personally identifiable health information outside the health care treatment entity that collected the information, if other Tier One authorization(s) do not apply;

and
- disclosure of personally identifiable health information, if adequate notice has not been given at the point of the initial authorization.

The Working Group identified a limited number of circumstances in which personally identifiable health information may be disclosed without patient authorization. These include:
- when information is required by law, such as for public health reporting;
- for oversight purposes, such as in fraud and abuse investigations;
- when compelled by a court order or warrant; and
- for research, as described in Principle 8 below.

7. Health care organizations should establish policies and review procedures regarding the collection, use, and disclosure of health information.

An organization's confidentiality policies and procedures should be coherent, tying together authorization requirements, notice given to patients, safeguards, and procedures for accessing personally identifiable health information. Organizations should also establish review processes that ensure a degree of accountability for decisions about the use and disclosure of personally identifiable health information. During such a process organizations might, for example, wish to determine routine procedures and special procedures for some areas of health care where medical information is considered highly sensitive to the patient.

8. Health care organizations should use an objective and balanced process to review the use and disclosure of personally identifiable health information for research.

For some areas of research, it is not always practical to obtain informed consent and, in some cases, a consent requirement could bias results. Recognizing this, the Working Group advises that patient authorization should not always be required for research. However, any waivers of informed consent should only be granted through an objective and balanced process.

Currently, any federally funded research is subject to the "Common Rule," where an Institutional Review Board (IRB) is required to make a determination about the need for informed consent. An IRB can choose to give a researcher access to personally identifiable health information with or without informed consent. But some research falls outside the scope of federal regulations. In such circumstances, health care organizations should use a balanced and objective process before granting researchers access to personally identifiable health information.

9. Health care organizations should not disclose personally identifiable health information to law enforcement officials, absent a compulsory legal process, such as a warrant or court order.

Federal privacy laws generally require that some form of compulsory legal process, based on a standard of proof, be presented in order to

disclose to law enforcement officers. Law enforcement access to health information should be held to similar standards. In some instances, however, government officials may access health information with legal process for the purposes of health care oversight. In these instances, the information obtained should not be used against the individual in an action unrelated to the oversight or enforcement of law nor should the information be re-disclosed, including to another law enforcement agency, except in conformance with the privacy protections that have attached to the data.

10. Health privacy protections should be implemented in such a way as to enhance existing laws prohibiting discrimination.

Currently, there are state and federal laws that prohibit discrimination on the basis of a person's health status in areas such as employment or insurance underwriting. Confidentiality policies should be implemented in such a way as to enhance and complement these protections. In effect, privacy can serve as the first line of defense against discrimination, creating a more comprehensive framework of protection.

11. Strong and effective remedies for violations of privacy protections should be established.

Remedies should be available for internal and external violations of confidentiality. Health care organizations should also establish appropriate employee training, sanctions, and disciplinary measures for employees and contractors who violate confidentiality policies.

The 11 principles outlined above focus on information gathered in the context of providing patient care and are written to establish a broad framework for the use and disclosure of health information. Although the Working Group recognizes that the need for privacy protections in other areas is no less urgent, this consensus document does not address the following areas:

- special considerations about the needs of minors;
- information that locates an individual in a particular health care organization (sometimes referred to as "directory information");
- information provided to spouses, dependents, and other next of kin;
- public health reporting;
- fraud and abuse investigations; and
- the appropriate relationship between state and federal law.

These 11 principles are designed to serve as a baseline for establishing patient privacy protections. While we all agree that health information, used in the right hands and with the right safeguards, can lead to improved health and advances in research, this information should not be used with disregard for patient privacy. Patients need to know that adequate protections are in place to protect their health information. Our hope is that these principles will go a long way towards establishing appropriate protections and, in the process, help build public trust and confidence in our health care system.

Background and Overview

BACKGROUND AND OVERVIEW

Confidentiality has long has been an essential element of the relationship between patients and health care professionals. But contrary to popular belief, the information people share with their doctors has never remained completely private—initiatives to improve individual and community health depend on accumulation of, and access to, medical records and other patient information.

The often uneasy interplay between protecting privacy and improving quality and access has been heightened by the rapid transition to a managed-care-dominated health care delivery system and increased use of information technologies. Over the years, the number of health care organizations handling patient data has grown significantly. The growth of integrated delivery systems has led to the development of integrated databases of personal health information. With access to this data, people are discovering new and often improved ways to deliver effective care, identify and treat those at risk for disease, conduct population-based research, assess and improve quality, detect fraud and abuse, and market their services. Not surprisingly, these uses may raise concerns about the ability to keep information private. Some people fear that there is an increased risk that information will "leak out," or that the information may be shared—even for legitimate purposes—with people who personally know the subject of the information.

Today, some people face a conflict over whether to share information with their health care providers or avoid seeking care in order to shield themselves. When people do not fully participate in their own care, they risk undiagnosed, untreated conditions. In turn, if the information collected by health care providers and health plans is not complete and accurate, it will be less reliable for research and public health initiatives. Ultimately, the public's fear and anxiety over the loss of privacy can threaten the very initiatives meant to serve them.

Health privacy has often been looked at as a "balancing process"—weighing the value of disclosure against the value of privacy to an individual. This approach, however, may not always serve the interests of either patients or health care providers. Rather than weighing these interests, the Health Privacy Working Group sought to *integrate* privacy protections as part of information practices. Strong privacy protections can help to build patient trust and insure that where information is shared, it is complete and reliable.

Privacy-Protective Behavior

Many people fear their personal health information will be used against them: to deny insurance, employment, and housing, or to expose them to unwanted judgments and scrutiny. After all, the information people share with their doctors is among their most sensitive. Medical records include family history, personal behaviors and habits, and even subjective information on mental state.

Best Principles for Health Privacy

Uses of health information often extend beyond patients' current knowledge and expectations, giving rise to a profound sense of anxiety, especially when the uses are inconsistent with the original purpose for which the information was gathered.

A national survey released in January 1999[1] found that one in five people believes that his or her personal health information has been used inappropriately, without their knowledge or consent. More striking, one in six Americans engages in some form of privacy-protective behavior to shield themselves from what they consider to be harmful and intrusive uses of their health information. To protect their privacy and avoid embarrassment, stigma, and discrimination, some people withhold information from their health care providers, provide inaccurate information, doctor-hop to avoid a consolidated medical record, pay out-of-pocket for care that is covered by insurance, and—in some cases—avoid care altogether.

The 1999 survey is supported by earlier research on privacy. Decades of survey research conducted by Louis Harris & Associates document a growing public concern with privacy and the protection of personal health information.[2] The 1995 Louis Harris poll found that 82% of people were concerned about their privacy, up from 64% in 1978. Nearly 60% of the public have at some point refused to give information to a business or company out of concern for privacy, up from 40% in 1990.

Benefits and Risks of Technology

The physical limits of the paper-based medical record itself have provided a modicum of protection against broad disclosure, but may also prevent providers, researchers, and others from getting information quickly and efficiently. Paper records are burdensome: different pieces of an individual's medical information can be kept in several different places, patient histories are recorded at almost every visit, notes are written by hand, and important information can be buried in a chart. Consequently, it has often been expensive and difficult to access needed information.

The increased use of new information technologies stands to offer many public health benefits. Information maintained in electronic form can be more efficiently collected, sorted, analyzed, and transmitted. As such, it can be accessed more easily for direct patient care, to coordinate care, and in emergency circumstances; it can be analyzed for population-based trends and may serve to reduce administrative costs by more easily transmitting information for the purposes of payment, referrals, and other functions.[3]

In terms of patient privacy, there are additional benefits: in many ways electronic health information may be more securely protected than paper records by limiting access, monitoring

[1] California HealthCare Foundation, *National Survey: Confidentiality of Medical Records* (January 1999). The survey was conducted by Princeton Survey Research Associates. Top-line results are available at http://www.chcf.org/conference/survey.cfm.

[2] Louis Harris & Associates, *Harris-Equifax Consumer Privacy Surveys* (published in 1992, 1995 and 1996). See also Louis Harris & Associates *Health Information Privacy Survey* (1993). All surveys were conducted for Equifax, Inc.

[3] See Paul Clayton, "Technical Measures for Protecting the Confidentiality of Computer-based Health Records," in *Protecting the Confidentiality of Patient Information in a Rapidly Changing Health Care System: Summary of a National Conference*, Appendix D (Health Systems Research, Inc. eds., 1998). The conference was sponsored by the Robert Wood Johnson Foundation, held January 14, 1998 in Washington, D.C.

users, and stripping data of personal identifiers before it is shared with third parties. At the request of the National Library of Medicine, the National Research Council conducted a study on privacy and security of health care information. Their report, published in 1997, found that the technology to protect data is readily available and not particularly costly. Still, there are few incentives to use privacy-enhancing technologies.[4]

Ultimately, while technological security measures can greatly improve patient privacy, they do not in and of themselves resolve the larger policy questions about how data should be used, shared, and exchanged. The technology can help to protect information, but only privacy policies—articulated in laws, regulations, and organizational policies—can articulate what limits are appropriate.

National Attention to Health Privacy

National attention to medical privacy is not new: as early as 1973 there were calls for increased attention to the privacy concerns presented by the use of computers in the health care industry. In 1976, the federal Privacy Protection Study Commission, created by the Privacy Act of 1974,[5] issued a report that included a section on the confidentiality of health information, with particular attention to insurance companies.[6] The commission noted that health care providers were losing control of patient records due to increasing population mobility, changes in the medical profession, and increasing demand for access to medical records by third parties. The commission's recommendations sparked a congressional effort to enact a medical privacy bill, but the effort failed.[7]

Since then, there have been a number of reports devoted to the promise of, and the challenges presented by, electronic health data.[8] Professional associations such as the American Medical Association, the American Psychiatric Association, the National Association of

---

[4] National Research Council, *For the Record: Protecting Electronic Health Information* (Washington DC: National Academy Press, 1997).

[5] Privacy Act of 1974, 5 U.S.C. § 552a (1988).

[6] Privacy Protection Study Commission, *Personal Privacy in an Information Society* (Washington DC: 1977).

[7] Also of note is the Supreme Court's decision in *Whalen v. Roe*, in which the Court addressed the privacy issues posed by a New York state law that required doctors and pharmacists to report to a state agency the names of patients who were prescribed controlled drugs. Although the Court ruled that the state law and computerized patient database did not violate patient privacy, it did so only after finding that the law contained extensive confidentiality and security safeguards to protect against unauthorized use and disclosure of sensitive health information. The Court also acknowledged that the Constitutional privacy "right to be let alone" includes "the individual interest in avoiding disclosure of personal matters," noting they were "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized databanks or other massive government files." Whalen v. Roe, 429 U.S. 589 (1977)

[8] Of particular note are: Richard S. Dick and Elaine B. Steen, Committee on Regional Health Data Networks, Division on Health Care Services, Institute of Medicine, *The Computer-Based Patient Record: An Essential Technology for Health Care* (Washington DC: National Academy Press, 1991); Office of Technology Assessment, U.S. Congress, *Protecting Privacy in Computerized Medical Information*, OTA-TCT-576 (Washington, DC: U.S. Government Printing Office, September 1993); Molla S. Donaldson and Kathleen N.

Social Workers, and the American Hospital Association have all adopted policies on protecting patient privacy. Other health care entities are moving forward to evaluate the need for new policies and security safeguards that address patient confidentiality, with particular attention to health information maintained in electronic format.

Nevertheless, state and federal laws have not kept pace with new health care delivery systems and new technology. Federal laws that apply in select circumstances include:

- Drug and Alcohol Abuse Regulations, which provide significant protections for people who receive drug and alcohol treatment at federally funded clinics;[9]
- Privacy Act of 1974, which provides protection for personal information collected and held by the government.[10]

The 1996 Health Insurance Portability and Accountability Act (HIPAA) includes a provision mandating that either Congress or the Secretary of Health and Human Services (HHS) establish an enforceable privacy regime to protect personally identifiable health information.[11] In HIPAA, Congress set itself a time limit of August 1999 for enacting a health privacy law. If Congress fails to act by that time, the secretary is required to promulgate health privacy regulations by February 2000.

To provide some guidance for legislation, HIPAA required the secretary to submit to Congress her blueprint for health privacy legislation. In September 1997, Secretary Shalala issued a set of recommendations to Congress to "enact national standards that provide fundamental privacy rights for patients and define responsibilities for those who serve them."[12] In her report, Secretary Shalala concluded that "without safeguards to assure that obtaining

Medicine, *Health Data in the Information Age* (Washington DC: National Academy Press, 1994); and Committee on Improving the Patient Record, Division of Health Care Services, National Research Council, *For the Record: Protecting Electronic Health Information* (Washington DC: National Academy Press, 1997).

9 42 U.S.C. Sec 290dd-2 (1988). Federal law does provide substantial privacy protection for people who receive drug and alcohol treatment at federally-funded clinics. The law's regulations apply strict confidentiality rules to oral and written communications of patient records, including "the identity, diagnosis, prognosis, or treatment of any patient."

10 5 U.S.C. 552a. The Act prohibits federal agencies from disclosing identifiable information without an individual's "prior written consent," except if the disclosure is "consistent with" the purposes for which the information was first collected. The Act also gives people the right to see, copy, and correct their records. The Privacy Act applies to identifiable health information maintained by the federal government, including records collected for Medicaid and Medicare recipients, and records of patients in federally funded hospitals. In addition, the Department of Veterans Affairs is bound by confidentiality rules covering treatment of drug and alcohol abuse, HIV, and sickle-cell anemia.

11 Health Insurance Portability and Accountability Act of 1996, P.L. 104-191. Also known as Kassebaum- Kennedy.

12 Secretary of Health and Human Services, *Confidentiality of Individually-Identifiable Health Information* (September 11, 1997). Recommendations submitted to the Committee on Labor and Human Resources and the Committee on Finance of the Senate; and the Committee on Commerce and the Committee on Ways and Means of the House of Representatives pursuant to Section 264 of the Health Insurance Portability and Accountability Act of 1996. (Hereinafter "Shalala Report")

health care will not endanger our privacy, public distrust could turn the clock back on progress in our entire health care system."[13]

Formation of the Health Privacy Working Group

Either through legislation, government regulation, or self-regulation, there will be significant developments with regard to health privacy in the next few years. Such developments will have a profound impact on many aspects of health care and health-related endeavors. While there is a growing body of information that speaks to patient confidentiality, this body of work remains somewhat fragmented—there is no consensus document that reflects "best principles" for health privacy agreed upon by a broad cross-section of the health care and consumer communities.

To meet this need, in June 1998 the Health Privacy Project convened the Health Privacy Working Group with the mission of achieving common ground on "best principles" for health privacy and identifying a range of options for putting those principles into practice.

The Working Group is comprised of diverse stakeholders in the health care and consumer communities. Members of the Working Group include: disability and mental health advocates; health plans; providers; employers; standards and accreditation organizations; and experts in public heath, medical ethics, information systems, and health policy. (See list of members on inside front cover and biographies in Appendix B.)

"Best Principles" for Health Privacy

The Working Group developed 11 principles. The intention is for the principles to be read—and implemented—as a whole. In many instances, the Working Group drew on the work of other organizations and commissions and the report credits those bodies where applicable.

The principles represent significant compromises between Working Group members. They should be seen as the workable common ground among diverse interest groups. As such, the principles reflect protections that should be considered when implementing comprehensive patient privacy policies and practices. There are a number of instances where the report flags areas for further consideration on the part of individual entities. The report also reflects the areas where Working Group members expressed a need for either a range of options or where consensus was not reached.

At every point, the Working Group sought to set appropriate limits on the use and disclosure of personally identifiable health information, while maintaining access in ways that can enhance health care. Again, the Working Group approached the issue of health privacy with an eye toward integrating privacy protections so that appropriate and necessary uses of health information could be assured, without compromising patient trust in the health care system.

Finally, the principles were written with an eye toward multiple constituencies, such as health care organizations, policy makers,

[13] Shalala report, pp 1-2.

consumer and disability advocates, and patients. Given the approaching HIPAA deadline for legislation or regulations, the Working Group was especially sensitive that the positions taken in this document might be translated into a legislative context. It should be understood that the principles do not necessarily represent the legislative or policy agenda of individual members of the Working Group, or the organizations/constituencies that they represent. In the course of developing the principles, there were instances in which members agreed on a particular "best practice," but did not think that the practice should be mandated by law.

Scope of Principles

In order to make the most significant contribution to the on-going national dialogue on health privacy, the Working Group chose to focus on information gathered in the context of providing patient care. The report specifically addresses information gathered and used in the treatment and health insurance context.

Members recognized that there are many more instances in which health information is collected and exchanged and the need for privacy protections in those contexts is no less urgent. A mailing list or a grocery store purchase, for example, could reveal a person's medical condition. Even more information is gathered in surveys and on-line discussion groups. The principles might be applied to information gathered in these and other contexts, but members did not intend for the principles to be used in those contexts without further analysis.

The principles are also written to establish a broad framework for the use and disclosure of health information. However, a number of areas fell outside the scope of the Working Group's focus, including:

- special considerations about the needs of minors;
- information that locates an individual in a particular health care organization (sometimes referred to as "directory information");
- the development and use of master patient indices to locate information on individuals;
- information provided to spouses, dependents and other next of kin;
- public health reporting; and
- fraud and abuse investigations.

Finally, this report does not address one of the issues that has proven quite difficult in the political arena: the appropriate relationship between state and federal privacy laws. The principles outlined in this report should go a long way towards helping health care entities and organizations to establish a framework to protect the confidentiality of personally identifiable health information. In that light, the Working Group has outlined a set of "best principles" to be implemented along with the requirements of state and federal law.

The Working Group recognizes, however, that state and federal laws are critical to bolstering and solidifying protections for personally identifiable health information. Where state and federal laws are weak, it may impair the ability of health care organizations to effectively protect health information, thereby making patients vulnerable to the misuse of the information. Current state laws vary widely in terms of the protections given to health information. The practical impact of the existing patchwork of inconsistent—and often inadequate—state law is that a health care organization may share information across state lines, but cannot trust that the information will receive adequate protections in the receiving state.

National health care delivery and payment entities are pressed to establish a more consistent privacy approach. At the same time, many consumer and disability rights groups want to insure not only that there are baseline protections across state lines, but also that heightened protections may be put into place where needed.

The Working Group did not agree on whether any federal health privacy law—if enacted—should preempt states from passing stronger laws in the future. As Congress moves to meet the HIPAA deadline, this issue will need to be resolved in the political arena.

The Working Group's aim is to recommend and promote these best principles so that—in the absence of a state or federal law—they can be translated into "best practices" to foster trust and confidence in our nation's health care system.

Principle #1

FOR ALL USES AND DISCLOSURES OF HEALTH INFORMATION, HEALTH CARE ORGANIZATIONS SHOULD REMOVE PERSONAL IDENTIFIERS TO THE FULLEST EXTENT POSSIBLE, CONSISTENT WITH MAINTAINING THE USEFULNESS OF THE INFORMATION.

This first—and overarching—principle is intended to create incentives to use information that does not identify individuals. Generally, the use and disclosure of information that does not identify individuals is not considered to compromise patient confidentiality. As such, users of non-identifiable health information should not be held to the same authorization requirements, standards or safeguards as users of information that identifies individual patients.

The full benefits of this principle will likely be realized primarily with electronic and automated records. In a paper-based environment, it is much more difficult and costly to remove, mask, or encrypt personal identifiers. Paper-based records will therefore more often remain personally identifiable.

Health Information Exists on a Continuum of Identifiability

Personally identifiable health information is indispensable for many activities, including the direct provision of patient care. There are many situations, however, when personal identifiers are not necessary for the success of the project or activity. Where health information does not identify individuals, concerns about privacy are greatly reduced.

Technology presents new opportunities to allow for greater access to health information—without compromising patient confidentiality—by removing, encrypting, or masking information that identifies individuals.

It is not, however, practically possible to ensure that all information is anonymous in all circumstances. Health information exists on a continuum, ranging from information that is fully anonymous to information that directly identifies an individual. Depending on the context, the same information elements may either be anonymous or may identify individuals.

The following scenarios highlight the complexity involved in making a determination about whether information is truly anonymous. At first glance, large data sets that do not contain names, social security numbers, and home addresses provide a high level of anonymity for the individual data subjects. When linked with other data, however, a person may be able to identify individuals. Conversely, in a small data set, an otherwise innocuous identifier

(such as place of birth) may identify an individual to people within an organization or community.[14]

Recommendations

In the context of providing patient care, personal identifiers will likely be necessary. Also, the ability to link de-identified medical information back to individuals is extremely important in some circumstances. However, there are many instances where personal identifiers can be removed. Organizations should have some flexibility and discretion in determining which individual identifiers are necessary for specific projects, and the extent to which they are able to remove individual identifiers.

At the same time, laws, regulations, and organizational policies should create strong incentives to remove personal identifiers wherever possible. Perhaps the strongest incentive to remove personal identifiers is that where organizations choose to use and disclose non-identifiable health information, they should not be subject to any of the requirements that apply to personally identifiable health information. With regard to non-identifiable health information that is encrypted or linkable to personal identifiers, the information is considered non-identifiable only if the user does not have the capacity to re-link the information. Once re-linked, the information is once again considered personally identifiable.

Data users will have to weigh many considerations in determining the possibility and practicality of using privacy-enhancing technologies, such as encryption. It may or may not be appropriate to anonymize health information. Moreover, even where it is possible to use anonymous information, it may be cost-prohibitive or, in the case of paper records, time consuming as well.

In many situations, it is likely that the data user may not be able to guarantee that the information is truly anonymous, i.e. that there is no possibility of identifying the individual. Health care organizations will have to make a determination about the level of risk to patient confidentiality and the risk to the project in removing identifiers. Where information is being made available to the general public, for example, the organization should take additional precautions in determining whether information is anonymous. Conversely, within the health care setting, a health care organization may want to preserve the ability to link back and re-identify information, as may be the case with some research projects.

Overall:

- Patient consent is not necessary for the use or disclosure of non-identifiable health information.
- Health information should be made as non-identifiable as possible at the earliest opportunity as consistent with the purpose for which the information will be used.
- Health care organizations should make a determination about the need for personally identifiable health information in advance of the use or disclosure of health information.

[14] Latanya Sweeney, "Weaving Technology and Policy Together to Maintain Confidentiality," 25 *Journal of Law, Medicine, & Ethics* 98 (1997).

Principle #2

Privacy protections should follow the data.

Health information will be used and shared for a variety of purposes. Data holders have an ethical responsibility to maintain public trust by treating health information in a confidential manner and should be held accountable for the ways in which they use, maintain, and disclose personally identifiable health information. Health information that identifies individuals should be subject to consistent requirements, regardless of the entity holding the data.

Recipients of health information should be bound by the protections and limitations attached to the data at the initial point of collection by existing or subsequent authorizations. In effect, the protections attached to the data at its source flow with it unless there is another authorization with varying protections. Responsibility for adhering to these obligations is based on a chain-of-trust model, which requires that agents, contractors, and receiving entities without their own authorization "step into the shoes" of the disclosing entities.

In practice, this principle requires that:

- Where personally identifiable health information is disclosed, the disclosing entity should condition disclosure, or write it into the disclosure agreement, that personally identifiable health information will only be used for the purposes identified and will not be further disclosed either without patient consent or other limitations by which the disclosing entity is bound.

- Recipients of health information may not re-disclose health information in personally identifiable form without specific, voluntary patient authorization for purposes outside existing authorizations or enumerated exceptions. Recipients should not use or disclose such information unless expressly permitted by an existing authorization.

This principle will need to be implemented closely with the principle that addresses authorization requirements (Principle #6). Consider the following scenario: a health plan secures a patient's authorization for the use and disclosure of health information for the purposes of treatment, payment, and business necessity. A member of the health plan may then visit a hospital. The hospital may request information from other providers, and from the health plan and may create new health information. The hospital may also have need to use and disclose the patient's information for other purposes unrelated to the health plan's needs, such as for their own accreditation and peer review activities. Those uses should not be considered "independent" because they fall under the kinds of activities the patient authorized initially.

Conversely, any recipient of health information that is not acting within the bounds of an existing authorization will have to secure a separate, independent authorization.

Principle #3

AN INDIVIDUAL SHOULD HAVE THE RIGHT TO ACCESS HIS OR HER OWN HEALTH INFORMATION AND THE RIGHT TO SUPPLEMENT SUCH INFORMATION.

Individuals should have the right to access and supplement their own health information so that they can make informed health care decisions and correct errors where appropriate. Access to audit trails and other records of disclosure can also help people understand how their health information is used and who has had access to their health information and may assist with remedying inappropriate disclosures.

Patient Access to Personally Identifiable Health Information

More than half the states currently provide people with the right to access and copy their medical records. The Health Privacy Working Group believes that patients should have access to their own medical information when it identifies them individually. Specifically:

- Individuals should have the right to see and copy their own medical records, including an accounting of disclosures, when such accounting is maintained.
- Data holders may not refuse inspection because they are owed money by the individual requesting inspection.
- Data holders may charge a reasonable fee for copying records or may provide secure on-line access to records.
- Minors who are legally able to consent to treatment should be afforded all rights to inspect and copy medical records.

Some health care organizations that have implemented audit trails currently allow patients to inspect the audit trail along with the medical record. Such patient access may require some time and effort on the part of a health care organization to help the patient understand an audit trail because the report will likely be coded, lengthy, and detailed. The Working Group was not in agreement about whether patients should have routine access to audit trails, but felt that allowing patients access in cases where there is a concern about improper disclosure could provide increased accountability.

Denial of Access

Access to personally identifiable health information may be denied to the subject of the information if:

- the disclosure could reasonably be expected to endanger the life or physical safety of any individual;
- the information identifies a confidential source;
- the information is compiled principally in connection with a fraud investigation or other criminal investigation and the investigation is not yet complete; or

- the health information was created as part of an individual's participation in clinical research, the research is not yet complete, and the individual was notified in advance about their rights to access information.

Where access has been denied, the health care organization should make a determination as to whether a portion of the medical record can be made available to the patient or a designated third party.

Supplementation of Medical Records

An individual should have the right to supplement his or her own medical record. Supplementation should not be implied to mean "deletion" or "alteration" of the medical record. An individual should not be able to modify statements that document factual observations or the results of diagnostic tests or to amend the record as to type, duration, or quality of treatment the individual believes he or she should have been provided.

The focus on a right to *supplement* the record—as opposed to a right to *amend* the record—may serve to better protect patients. Where an error in the record has been made, the supplementation can serve as historical documentation. Where the patient and provider disagree, such disagreements can also be reflected in the record.

Principle #4

Individuals should be given notice about the use and disclosure of their health information and their rights with regard to that information.

Individuals should be given easy-to-understand written or on-line notice of how their health information will be used and by whom. Only with such notice can people make informed, meaningful choices about uses and disclosures of their health information. Adequate notice can also help to build trust between providers, health care organizations, and patients in so far as it removes any element of surprise about the use and disclosure of health information.

Components of Notification

Notice should be given at the point of application for health benefits, enrollment in a health plan or health insurance company, and at an initial encounter with a provider, if outside the scope of other notifications.

Notice should include the following elements:

- *Collection of Information*: How information will be collected and the information source, such as a medical record, treatment notes, and information from third parties.

- *Uses and Disclosure of Information*: How the entity will use the information, and how, when, and for what purposes the entity will request patient authorization.

- *Patient Right to Access Health Care Information*: What

information the patient is permitted to inspect and copy and how to access such information.

- *Patient Right to Prevent or Limit Disclosure*: Where there is a legal requirement or an organization's policy permits, patients should be notified about the steps available, if any, to limit access and the consequences, if any, of refusing to authorize disclosure. Such notice should include the rights of patients who choose to pay out-of-pocket for their care. In cases where a health care organization does not permit patients to prevent or limit disclosure, the health care organization should make that known in the notice provided to patients.

- *Organization policies*: The health care organization's policy for making disclosures with and without patient authorization, such as for research purposes, to law enforcement, for treatment purposes, etc.

- Any other information relevant to the health care entity's data practices.

Ultimately, patients should know what is being done with the information collected about them.

Principle #5

HEALTH CARE ORGANIZATIONS SHOULD IMPLEMENT SECURITY SAFEGUARDS FOR THE STORAGE, USE, AND DISCLOSURE OF HEALTH INFORMATION.

Appropriate safeguards should be in place to protect health information from unauthorized use or disclosure. The security safeguards do not mandate specific technical controls and are intended to be appropriate for use with electronic and paper records.

Rationale

As the 1997 National Research Council (NRC) report *For the Record* concluded, technology can be used to better safeguard personal health information in electronic form than it would be protected if on a piece of paper in a file drawer. Also, technology can be used to more efficiently anonymize and de-identify personal health information.

The Health Privacy Working Group discussed the trade-off between availability of data and confidentiality. While it is possible to afford high security protections to data, such security will also make it harder to access health information for legitimate and necessary uses. For example, if all health information is afforded the highest possible security protections, the data may not be readily available in emergency circumstances.

Requirement for Security Standards in HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the Department of Health and Human Services (HHS) to issue security standards for "all entities, regardless of size, involved with electronic health information pertaining to an

individual." HHS has circulated proposed rules that identify a security matrix to establish minimum requirements for security.[15] The matrix includes administrative procedures, physical safeguards, technical security services, and technical mechanisms. While the regulations will only apply to payers, providers, and electronic clearinghouses, all health care organizations should look to the regulations for guidance on technical and administrative safeguards.

The proposed matrix does not mandate specific technological controls, but requires organizations to make a determination about the level of risk involved in giving or denying access and in turn define what appropriate levels of control are warranted. The proposed regulations also place a heavy emphasis on administrative safeguards that underscore an organization's greatest vulnerability—the people who have access to identifiable information.

The Working Group agreed that it would be unwise to re-open discussion about security standards that are due to be finalized soon. There is, however, a specific nexus between confidentiality and security that needs attention. Security safeguards identify the *means* by which an entity may protect the privacy of health information. The safeguards as articulated in the HHS draft regulations do not establish who should have access and for what purposes and what a patients' rights are with regard to their health information. The specific safeguards outlined below are intended to supplement the matrix being finalized by HHS.

Recommended Safeguards

Overall, the implementation of security safeguards will be driven by the specific confidentiality policies, authorization requirements, state and federal law, and principles organizations adopt. Some safeguards, for example, are implied from the principles outlined in this report. For instance, the principle on authorization prohibits psychotherapy notes from being shared, except as required by a health oversight agency or public health authority, or with the explicit and voluntary authorization of the individual. Health care organizations will have to implement appropriate technical safeguards to ensure compliance with this principle.

The Working Group did not discuss specific security controls at great length. There were a number of safeguards, however, that were discussed in the context of "fair information practices." They include:

- Health care organizations should endeavor to limit access to personally identifiable health information on a need-to-know basis. Employers, for example, should endeavor to restrict access to personally identifiable health information strictly to those employees who need access for payment or treatment purposes.

- In keeping with Principle #1, health care organizations should remove personal identifiers to the fullest extent

[15] For the proposed rules and comments, see the administrative simplification website of the United States Department of Health and Human Services at http://aspe.os.dhhs.gov/admnsimp.

Principle #6

Authorization

possible and practical, consistent with maintaining the usefulness of the information.

- All disclosures of personally identifiable health information should be limited to the information or portion of the medical record necessary to fulfill the purpose of the disclosure.
- Health care organizations should maintain a record of disclosures of information that identifies an individual.
- Personally identifiable health information should be used within an organization only when such information is necessary to carry out the purpose of the activity, for purposes reasonably related to the purposes for which the information was collected, and for which the patient has been given notice.
- Organizations should consider whether they are able to provide patients with a greater degree of anonymity in certain circumstances through the use of opt-outs, pseudonyms, identification numbers, or tagging information for additional protections.

Tailoring Safeguards

As organizations adopt more sophisticated technologies, they should aim to build in the appropriate level of privacy protections.

Principle #6

PERSONALLY IDENTIFIABLE HEALTH INFORMATION SHOULD NOT BE DISCLOSED WITHOUT PATIENT AUTHORIZATION, EXCEPT IN LIMITED CIRCUMSTANCES. HEALTH CARE ORGANIZATIONS SHOULD PROVIDE PATIENTS WITH CERTAIN CHOICES ABOUT THE USE AND DISCLOSURE OF THEIR HEALTH INFORMATION.

The Working Group agreed that, as a general rule, patient authorization should be obtained prior to disclosure. At the same time, patient information needs to be shared for treatment, payment, and core business functions. The Working Group agreed that the patient need only provide authorization for these core, essential uses and disclosures once. Furthermore, a health care organization can condition the delivery of care or payment for care on receiving this Tier One authorization. All other activities outside this core group must be authorized separately by the patient and health care services should not be conditioned on receiving this Tier Two authorization. The Working Group also agreed that there are additional, limited activities—such as public health reporting and emergency circumstances—for which patient authorization should not be required.

Rationale

Today, most health care organizations require some form of patient authorization for the use and disclosure of health information. An authorization may be requested at the point of enrollment in a health plan, and/or when a patient sees a provider for the first time.

Typically authorizations are worded broadly enough to encompass many different kinds of activities. Additional authorizations may be collected for specific activities such as releasing a record to a new provider, for participation in a research study, or for obtaining life insurance. Some states also require additional and specific authorizations for specific conditions such as HIV/AIDS, drug and alcohol treatment, and mental health.

Patient authorization is a critical component of protecting patient privacy. Because the disclosure of health information can have significant consequences for individuals, they should have some control over the use and disclosure of personally identifiable health information.

Further, the process of obtaining patient authorization can also define an "initial moment" in which to educate patients and elicit special individual patient concerns about confidentiality. As a general rule, requiring patient authorization prior to disclosure can:

- bolster patient trust in providers and health care organizations by acknowledging the patient's role in health care decisions;
- serve as recognition that notice was given and the patient was aware of the risks and benefits of disclosure; and
- define an "initial moment" in which patients can raise questions about privacy concerns and learn more about options available to them.

At the same time, health information must be shared for a variety of activities in order to provide care, pay for care, and ensure the effective operation of the health care system. For some organizations, and especially networked delivery systems, it would be administratively burdensome and costly to obtain patient authorization prior to each use or disclosure.

The Working Group, therefore, agreed upon an authorization structure that allows for a health care organization to consolidate certain essential—or core—activities in a single, one-time authorization. Moreover, because these are critical—but limited—activities, the health care organization may condition the delivery of care or payment for care on receiving an authorization for these core treatment, payment, and business purposes. All other activities outside this core group should be authorized separately by the patient and he or she can refuse authorization without suffering any adverse consequences. The Working Group also agreed that there are additional, limited activities for which patient authorization should not be required. They are outlined in this report.

The basic framework here is a two-tiered authorization structure. Core activities are placed in Tier One, where the health care organization is given more discretion to make decisions about disclosure. In these circumstances, patient authorization functions as evidence that individuals have been given notice about information practices. For those activities that are not core, and therefore not

itemized in Tier One, patients are given the ability to control disclosures of their health information without the delivery of care or payment for care conditioned on the receipt of the authorization. In other words, for this Tier Two set of activities, signing an authorization is voluntary and optional.

It should be noted that in arriving at this structure, the Working Group considered other authorization models. The Secretary of Health and Human Services, for example, recommended a model in which the use and disclosure of identifiable information for treatment and payment would be exceptions to the authorization requirements. In effect, the patient would implicitly authorize the use and disclosure of information for select activities by virtue of enrolling in a health plan or presenting for care. The underlying assumption of the secretary's recommendations is that most patients do not read authorization forms and do not have a meaningful opportunity to object to a core set of disclosures. The secretary's intent was to lend greater value to the authorization process by ensuring that where an authorization is presented, it is truly voluntary and uncoerced.

However, the Working Group agreed that there is a value in requiring patient authorization even for the core activities where patient authorization is, in practice, a signed acknowledgment that the authorization has been read. Again, the authorization requirement can define a moment in which patients can assess their concerns about confidentiality and take actions—such as paying out-of-pocket for care or seeking care from a particular entity—to preserve the confidentiality of their health information.

The framework outlined below provides for a workable middle ground: it requires patient authorization, but allows health care organizations to deny treatment or payment if authorization is refused for the critical, Tier One activities.

Obtaining Patient Authorization

The organization disclosing health information is responsible for ensuring that the appropriate authorization is obtained prior to disclosure. The authorization for core Tier One activities may be obtained at the point of enrollment or at the time of treatment, after adequate notice of information practices has been given. The authorization should be considered valid until a patient leaves a plan or insurer, or changes providers. The authorization may be revoked at any time, with certain limitations.

Authorization from a policy-holder should not be understood to include authorization for all individuals covered in that policy. Health care organizations should obtain an authorization from each individual who is legally able to provide authorization and is covered by the insurance policy or is seeking care.

Tier One Authorization	Tier Two Authorization	Uses and Disclosures Allowed without Patient Authorization
Health care organizations can obtain a single consolidated authorization for all Tier One activities. Furthermore, the health care organization may refuse to provide treatment or to pay for care if a patient refuses to provide authorization.	Activities not listed under Tier One should be authorized separately. A patient can refuse authorization without suffering negative consequences. This list is illustrative of the kinds of activities that health care organizations may place in this category— it is not intended to be a finite list.	There are a limited number of circumstances in which personally identifiable health information may be disclosed without patient authorization.
Treatment: The sharing of information necessary for the direct provision of care to a specific patient *Payment:* The sharing of information necessary to provide payment for health care. *Business Necessity*: Business necessity is understood to include the sharing of information necessary for the administrative and technical operation of a health care organization. **Note:** Where a patient self-pays, he or she can refuse to authorize disclosure to a payer.	All activities not covered in the Tier One authorization or in the exceptions to patient authorization. The activities listed below are illustrative and not a finite list of activities that need additional authorization. For purposes of marketing. For the disclosure of psychotherapy notes. For disclosure of personally identifiable information to an employer, except where necessary to provide or pay for care. For disclosure of personally identifiable health information outside the organization or agency. (Note: agents and contractors are not considered to be outside the agency.) For the disclosure of personally identifiable health information, if adequate notice has *not* been given at the point of the initial authorization.	*If the information does not identify an individual*: Patient authorization is not needed for the use and disclosure of information that is anonymous. *When required by law*: Health information may be used and disclosed without patient authorization when specifically required by law, such as for public health reporting. *For oversight purposes*: Health information may be used and disclosed without patient authorization for use in legally authorized fraud and abuse investigations. *If compelled by a court order:* Health information may be used and disclosed without patient authorization if required by compulsory legal process, such as a warrant or court order. *For research*: If consistent with Principle #8.

Principle #6

Authorization

Authorization Requirements for Core Activities: Tier One

The Working Group agrees that it is possible to establish a "one-time," durable authorization for those activities that are necessary and routine: namely, activities that are directly tied to treatment, payment, and business necessity.

There was considerable discussion about what constitutes a "core" activity. Members wanted to be broad enough to accommodate a rapidly changing health care system—activities not considered essential now may be in the future. At the same time, because authorization for core activities is non-negotiable from the patients' perspective, it was important to limit the range of activities to those that are truly necessary for the delivery of care and effective operation of the health care system.

Treatment

Treatment is understood to be the direct provision of care to a specific patient. In most circumstances, it is desirable for the treating physician to have access to the complete medical record. Health care providers may also share information about individual patients in the course of treatment—in consultation with another provider, in a referral to another provider, or in follow-up activities. In a managed care context, treatment is understood to include the sharing of information necessary to coordinate care between providers in a common network or integrated delivery system.

There was considerable discussion about the scope of "treatment"—and whether some activities that might be considered treatment may need special consideration in terms of the authorization requirements. Disease management, for example, is defined by "a systemic, population-based approach to identify persons at risk, intervene with specific programs of care, and measure clinical and other outcomes." In so far as the disease management program is addressing the health care concerns of specific individuals, it is considered "treatment," and needs to be conducted with information that identifies individuals. But disease management may also include an administrative, quality, or research component not directly associated with an individual.

Some consumer concerns about disease management programs are that they are often contracted out to third parties; may include a marketing or promotional component; or that patients may not receive adequate notice about the program.

At the same time, there are many benefits to disease management programs. Where the program is conducted to bring patient care up to "best practices," the program stands to improve outcomes and reduce costs. Moreover, because the health plan or payer may be assuming financial risk for the patient, it is in their interest to identify and manage high-risk patients.

Disease management may be considered a Tier One activity, when it is conducted as part of a treatment regimen. The Working Group, however, is not recommending specific authorization requirements

for disease management programs given the differences in disease management programs as they are currently conducted. The Working Group does recommend that when conducting disease management programs, health care organizations should consider:

- the sensitivity of the medical condition being addressed;
- whether patients were given notice up-front about the existence of disease management programs;
- the manner in which patients are being contacted once enrolled in the program; and
- the practicality of allowing patients the ability to opt-in or opt-out of the program.

Disease management programs are still in an early stage of development, which presents particular challenges with regard to notification and authorization. A patient might be treated for a certain condition—such as high blood pressure—for many years when a new program becomes available. The result is that existing authorization forms and notification may not adequately address the new program. Some health care organizations have chosen to implement disease management programs through a provider. A physician's office may make contact with the patient or approve the contact with the patient through another medical professional. In such circumstances, specific patient consent may not be required, but the provider can help to make decisions about whether the use or disclosure is appropriate.

Restricting Use and Disclosure of Psychotherapy Notes

The Working Group agreed that where psychotherapy notes are separate from the medical record, they should not be shared without specific patient consent. Unlike information shared with other providers for the purposes of treatment, the psychotherapy notes are more detailed and subjective and are subject to unique rules of disclosure.[16] In addition, the notes are not ordinarily shared with the individual patient. A tension is created if the notes are shared beyond the provider when they are not made available to the patient. The notes are of primary value to the specific provider and the promise of strict confidentiality helps to ensure that the patient will feel comfortable disclosing information essential to the therapeutic relationship.

The phrase "psychotherapy notes" includes only the personal notes taken by a mental health professional. The notes do not include diagnostic and treatment information, signs and symptoms, or progress notes, which may be shared in the same manner as other clinical information.

---

[16] Jaffee v. Redmond, 116 S. Ct. 1923 (1996). In *Jaffee v. Redmond*, the Supreme Court ruled that conversations and notes between a patient and therapist are confidential, and that the traditional doctor/patient privilege required that they be protected from compelled disclosure. The Court found that "[e]ffective psychotherapy depends on an atmosphere of confidence and trust, and therefore the mere possibility of disclosure of confidential communications may impede the development of the relationship necessary for successful treatment. The privilege also serves the public interest, since the mental health of the Nation's citizenry, no less than its physical health, is a public good of transcendent importance."

Principle #6

Authorization

Segregation of the notes by health care providers will be critical in implementing and enforcing these heightened privacy protections.

Restricting Disclosure for Treatment Purposes

While there are few authorization requirements for uses related to treatment, not all information collected in a treatment context should be made available to all practitioners. Information is only available on a need-to-know basis—it must be relevant to the care of the patient at that time. Access to a history of reproductive services, for example, would likely not be relevant if a patient were admitted for a sprained ankle. Decisions about whether information is relevant will have to be made within an organization and by individual providers. In emergency circumstances, for example, it may be assumed that the provider may have the ability to access the entire medical record. In other circumstances, the health care organization or provider may consider restricting access within a treatment context.

Patients may have the ability to restrict additional disclosures related to treatment, but such considerations should be made on a case-by-case basis between the health care provider and the patient.

There will be special situations in which patients will have specific concerns about the confidentiality of their health information. A patient may have friends or relatives who are employees of the health care organization. A patient may also be reticent to access care at all. Where fears about confidentiality may be a barrier to treatment, the health care organization may want to accommodate a patient's desire to use a pseudonym when seeking care or to more tightly control access and disclosure of an individual patient's health care information.

Health care organizations may also want to allow people the ability to limit disclosure for disease management and other programs intended to supplement care delivered by a physician. A patient may have concerns about receiving mail or a phone call at home. Such concerns may be more frequently associated with certain services, such as family planning and mental health treatment. The health care organization may choose to accommodate such concerns.

A health care organization will have to make a judgement about their capacity to accommodate a patient's desire to shield information, but should aim to provide greater anonymity through the use of pseudonyms, encryption, or other techniques to shield the identity of an individual.

Payment

Disclosure and use for payment purposes includes the sharing of information necessary to make payments for health care services. In addition, payment is understood to include:

- Utilization review: "A process to determine which health services are medically necessary and appropriate (and therefore, which services are covered under the health benefits contract)."[17]

[17] American Accreditation HealthCare Commission/URAC, *Survey of State Health Utilization Review Laws and Regulations,* p.9 (Washington D.C: 1999).

- Precertification: "The process of obtaining certification or authorization from the health plan for routine hospital admissions (inpatient or outpatient). Often involves appropriateness review against criteria and assignment of length of stay. Failure to obtain precertification often results in a financial penalty to either the provider or the subscriber."[18]

- Justification of charges and coverage determinations including medical necessity.

As always, disclosure should be limited to the amount necessary to process the claim. Where the payer is also the employer, only information necessary to process a claim should be shared in personally identifiable form with employer's benefits personnel. (See Principle #10 on discrimination.)

Restricting Disclosure for Payment Purposes

A patient may explicitly limit disclosure of personally identifiable health information to a payer if he or she pays for care out-of-pocket. It should be emphasized that where a patient self-pays, it only limits disclosure to a payer; the information may still be used for other Tier One activities.

Business Necessity

Business necessity is understood to include the sharing of information necessary for the administrative and technical operations of a health care organization. Not every health care organization will have the same management needs. While a health care organization may contract out for these services, they are activities that are conducted using "in-house," or member, information. Business necessity may include:

- Auditing: Reviews of services delivered and billing to them to assure compliance with fraud and abuse statutes.

- Credentialing: "Obtaining and reviewing the documentation of professional providers. Such documentation includes licensure, certifications, insurance, evidence of malpractice insurance, malpractice history, and so forth. Generally includes both reviewing information provided by the provider and verification that the information is correct and complete. A much less frequent use of the term applies to closed panels and medical groups and refers to obtaining hospital privileges and other privileges to practice medicine."[19]

- Accreditation: A voluntary review by private-sector organizations. Accreditation is looked to as an important measurement by payers. It may also be a requirement of participation in certain payment programs, such as Medicare.

- Quality assurance: The use of patient information to evaluate care for a particular population.

[18] Peter Kongstvedt, *The Managed Health Care Handbook, Third Edition* (Maryland: Aspen Publishers, 1996) at 1000. (Hereinafter "Kongstvedt.")

[19] Kongstvedt at 991.

- The creation of non-identifiable health information.

Many of these activities could be conducted with information that does not identify individual patients, but that may not always be practical, especially in a system that relies on paper medical records. Because consent for activities considered "business necessity" may be non-negotiable from the patient's perspective, the Working Group agreed that it was important to provide additional guidance to health care organizations about making a determination about the use of health information for these activities. Consideration should be given to the following questions:

- Is the activity necessary for the optimal performance of the organization?
- Is identifiable information necessary, or why is it impracticable to remove, mask, or encrypt personal identifiers? and
- Can patients withhold their consent for their identifiable information being used for any of the activities?

To the extent feasible, health care organizations should strive to educate patients about the use of their personally identifiable health information for purposes of business necessity. The organization's specific practices in this area should be clearly defined and incorporated into the notice provided to patients.

Restricting disclosures for business necessity

Based on the above standard, the health care organization should make a determination about whether patients have the ability to restrict disclosures. Health care organizations, however, should use information that is as non-identifiable as possible for these activities, where feasible.

Accommodating Sensitive Conditions

The Working Group determined that the two-tiered authorization structure was generally adequate. However, health care organizations may want to evaluate the need for additional authorization requirements for those conditions that have a history of stigma and discrimination.

A number of states have stringent authorization requirements for some health conditions. California, for example, requires specific patient authorization each time HIV/AIDS information is shared or disclosed, even between providers.[20] Massachusetts requires that an authorization for the disclosure of HIV/AIDS information be separate from other authorizations.[21] While the Working Group did not specifically endorse a more restrictive authorization model, certain organizations may want to consider additional models that provide heightened protections for their patient population.

The Working Group acknowledged that health care organizations should consider whether unique authorization requirements should be

[20] Cal. Health and Safety Code § 120985 (a) (Deering 1997).

[21] Mass. Ann. Laws ch.111, § 70F (West 1998).

established for highly sensitive information including information about HIV/AIDS and other sexually transmitted diseases, reproductive health, genetic information, abuse and neglect, drug and alcohol abuse, and mental health.

Additional authorization requirements may be particularly helpful in terms of allowing patients more control of the availability of information within an entity. A person with a stigmatized condition, for example, may not be willing to seek treatment if a relative or friend is an employee of the health care organization. Likewise, a public figure may need to seek care under a pseudonym.

Either by law or practice, some organizations require explicit authorization for the disclosure of certain "sensitive" information, even for treatment and payment. In these cases, a general, Tier One authorization is not adequate. In some circumstances, the authorization can be obtained from the patient. In others, the health care organization may ask the provider to authorize disclosure.

Patient concerns about confidentiality may center on the availability of personally identifiable health information to specific people: a certain provider, an employee, a payer, or the public. These additional authorization requirements could allow patients to have greater control of their health information without jeopardizing the delivery of care or business operations.

Finally, health care organizations should remain flexible in terms of what counts as a "sensitive condition." Emerging technologies, such as genetic testing, may present new confidentiality concerns. Even on an individual level, different conditions will be considered sensitive to different people. Family situation, care setting, and diagnosis can all affect how and whether individuals perceive their health information to be "sensitive." Health care organizations are encouraged to respond to individual concerns, and to revise authorization policies as necessary.

Authorization Requirements for Non-Core Activities: Tier Two

All activities not within Tier One fall into Tier Two which requires a separate, specific authorization from the patient. The delivery of care or payment for care cannot be conditioned on receiving this Tier Two authorization. A health care organization should receive separate authorization from each individual who is of legal age to consent to treatment.

Tier Two will include many activities. Additional and separate consent, for example, may be necessary for the following illustrative examples:

- For the disclosure of psychotherapy notes. (See earlier discussion: "Restricting Use and Disclosure of Psychotherapy Notes")

- For disclosure of personally identifiable health information to an employer, except where necessary to provide or pay for care. When information is shared with employers, it may not be used for promotion, hiring/firing, except as the

medical condition affects the person's ability to carry out the job even with reasonable accommodation.

- For disclosure of personally identifiable health information outside the organization or agency. (Note: agents and contractors are not considered to be outside the organization or agency. A health care organization, for example, may hire a company to suggest steps to improve the quality of care. If in the process of executing the contract, the company reviews patient information, it would not be considered a disclosure "outside the agency.")

- For the disclosure of personally identifiable health information, if adequate notice has *not* been given at the point of the initial authorization.

The list above is not intended to be comprehensive, but is illustrative of the kinds of activities that can be expected to require additional, specific patient authorization. Each health care organization should make a determination about the kinds of activities that it believes fall into this category.

Finally, for the most part, marketing activities conducted primarily for profit, and not tied to patient care, will require additional, specific patient authorization. There are some activities, however, that financially benefit the health care organization, but are aimed primarily at enhancing patient care. A health care organization may market its own services to members or patients. Such "grey areas" should be vetted through an organization's data review process (as articulated in Principle #7). The expectation is that:

- The organization will consider the direct benefits to the patient in determining whether specific, voluntary authorization is needed for the activity; and

- The organization will only market its own services, unless they receive specific patient authorization. A health plan, for example, should not share patient names with a pharmaceutical company who is looking to market a new medication, unless there is specific authorization. On the other hand, a health plan may market their own clinical services to patients who can be expected to benefit from the services.

Such activities should be disclosed to the patient as part of the notice of organizational policies (see Principle #4).

Uses and Disclosures Allowed without Patient Authorization

Finally, there are a limited number of circumstances in which the requirements for patient authorization can be waived, or in which personally identifiable health information can be disclosed without authorization. For the most part, these exceptions are in areas in which there are existing mechanisms—such as legal requirements or regulations—that speak to the use of the data:

- *When required by law*: Health information may be used and disclosed without patient authorization when specifically required by law, such as for public health reporting.

- *For oversight purposes*: Health information may be used and disclosed without patient authorization for use in legally authorized fraud and abuse investigations.

- *If compelled by a court order:* Health information may be used and disclosed without patient authorization if compelled by a court order in a civil or criminal investigation.

- *For research*: Health information may be used or disclosed without patient authorization for the purposes of research, consistent with Principle #8.

- *If the information does not identify an individual*: Patient authorization is not needed for the use and disclosure of information that is non-identifiable. (See additional principles on the use of non-identifiable information and the internal data-review committee.)

The Relationship to Notice

In some respect, authorization for Tier One activities is an acknowledgment that notice has been given. Except when the patient pays for care out-of-pocket, there is little opportunity to object to certain uses or disclosures. The Working Group intends to solidify this connection by requiring additional authorization if notice has not been given. For example, if a health care organization started conducting disease management programs for the first time and had, therefore, not provided any notification to patients they would need to obtain patient authorization for participation or provide notice to patients, about the initiation of the programs. For new patients or new enrollees, the organization could simply incorporate the program in the notification and Tier One authorization.

By more tightly connecting the authorization and notice requirements, the Working Group seeks to ensure a more educated patient population and to minimize uses of health information that are not known to the patient.

The Relationship to Safeguards

The tiers speak only to authorization requirements. To fully appreciate the impact of the authorization requirements, they must be implemented hand-in-hand with security safeguards (see Principle #5). While the authorization requirements will help individual patients control the disclosure of their health information, the security safeguards will place additional limits on the disclosure. Many security safeguards, for example, address patients' concerns about access within an entity, limiting the amount of information disclosed to third parties, and limits on re-disclosure.

Principle #7

HEALTH CARE ORGANIZATIONS SHOULD ESTABLISH POLICIES AND REVIEW PROCEDURES REGARDING THE COLLECTION, USE, AND DISCLOSURE OF HEALTH INFORMATION.

Every health care organization will use and disclose health information for different purposes. An organization's confidentiality policies and procedures should be coherent, tying together authorization requirements, notice given to patients, safeguards, and procedures for accessing personally identifiable health information. As such, health care organizations should:

- generate, review, and enforce confidentiality policies;
- implement minimum safeguards needed to make the policies operational; and
- review specific projects and procedures where there are ramifications for patient confidentiality.

Taking into consideration size, range of activities, and population base, organizations should establish a review process that oversees the above responsibilities. This may be accomplished through a specific committee designated to oversee confidentiality or through an existing committee, department, or individual (in the case of a small organization). For some areas it may also be appropriate to get input from members of the community, especially representatives of populations that would be affected by the policy.

Internal Review

An organization's confidentiality policies will help to set broad parameters to guide the use and disclosure of health information. For routine activities—such as patient care, billing, and quality assurance—the established policies and procedures are likely to be adequate. However, there will continue to be additional internal and external demands for health information or new projects that raise concerns about patient confidentiality.

The Working Group acknowledged that many requests for personally identifiable health information are necessary and valuable. Organizations should establish a review process that helps to insure accountability for decisions about the use and disclosure of personally identifiable health information. At a minimum, the review should:

- assess the need for information that identifies individual patients;
- weigh the benefit of the activity with the risk to patient confidentiality;
- make a recommendation on the need for patient authorization; and
- identify minimum required safeguards.

Where the health care organization has chosen to share information for a particular project, patients should have access to the decision on request. Ultimately, the internal review allows organizations a great deal of flexibility, while providing patients with an organizational mechanism to oversee information uses and disclosures. The intent here is to increase accountability for individuals and organizations that are using and disclosing personally identifiable health information.

Current Practices

This principle is in keeping with current professional recommendations and has been implemented in leading health care organizations. For instance, NCQA/JCAHO accreditation standards, to be implemented soon, require managed care organizations to designate "an internal review board to create and review confidentiality policies and to review practices regarding the collection, use, and disclosure of medical information."[22] Among the board's responsibilities are to:

- review all internal and external requests for using identifiable member data;
- determine levels of authorized user access to data; and
- establish mechanisms for adhering to specific member requests to limit access to data.

Intermountain Health Care of Utah has recently established a Data Access Committee that works specifically on issues of access to data for projects outside of the Institutional Review Board's scope. The Data Access Committee "recommends policy to IHC's Board of Trustees, and individually examines and acts upon all projects that fall into the definitional grey area between operations and research. The Data Access Committee reports directly to IHC's Board of Trustees. Its members include research scientists; experts in medical informatics; practicing clinicians; medical ethicists; a knowledgeable community member not associated with IHC or with other health care delivery or research; and senior managers from IHC's care delivery operations. As an extended quorum, all IRB chairpersons working within IHC also attend to discuss problems and recommend policy supporting IRB function throughout the IHC system. A full record of each meeting is generated and maintained." [23]

---

[22] Joint Commission on Accreditation of Healthcare Organizations and the National Committee for Quality Assurance, *Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment* (Washington, D.C.: November 1998). The full report is available on-line at http://www.ncqa.org/confide/tablcont.htm.

[23] *Confidentiality of Medical Information Hearing*, Senate Committee on Health, Education, Labor and Pensions, 104th Cong. (February 24, 1999) (statement of Brent James, Executive Director, Intermountain Health Care Institute for Health Care Delivery Research).

Principle #8

HEALTH CARE ORGANIZATIONS SHOULD USE AN OBJECTIVE AND BALANCED PROCESS TO REVIEW THE USE AND DISCLOSURE OF PERSONALLY IDENTIFIABLE HEALTH INFORMATION FOR RESEARCH.

The Working Group believes that it is important to create equity, fairness, and accountability in the application of confidentiality policies to research involving the use of personally identifiable health information. Such an across-the-board approach will provide more comprehensive confidentiality safeguards, as well as bolster the public's trust and confidence in research initiatives.

Currently, research that receives federal funding, or is conducted in anticipation of FDA approval, is subject to the "Common Rule,"[24] a federal regulation that requires that any use of "identifiable private information" be overseen by an Institutional Review Board (IRB). The rule was established for the purpose of supervising research and protecting "the rights and welfare of human research subjects."[25] Under the regulations, a researcher must obtain informed consent to use personally identifiable health information, unless the IRB approves a waiver or the research falls within one of the enumerated exceptions to informed consent.

Where the research is currently subject to IRB review, the Working Group agreed that consent requirements and security safeguards should continue to be addressed by the IRB. For research not currently subject to IRB review, health care organizations should either use an existing IRB or establish an objective and balanced review process to determine the need for informed consent and appropriate safeguards.

In all circumstances, health care organizations should ensure balance and accountability in decisions about the use of personally identifiable health information for research. Towards that end, all research—whether federally regulated or not—should be subject to a review process and the application of certain standards.

Structure: Balanced and Objective Review

Objective and balanced review can help to ensure that researchers anonymize information when possible and serve as a check on the legitimacy of the objectives of the research. Review may also be in the interest of the disclosing entity—it can help it to determine if the project is a good use of their resources, if the risk is minimal to the subjects, and if the project is of scientific merit.

Again, existing federal regulations require that certain research be approved by an IRB. The regulations specify that the IRB include at least one member who is not "otherwise affiliated with the

[24] 45 CFR part 46, subpart A, known as the "Federal Common Rule." The Food and Drug Administration's equivalent regulation is 21 CFR part 50 and 21 CFR part 56.

[25] Office for Protection of Research Risks, United States National Institutes of Health, *Institutional Review Board Guidebook* (1993) at 1-1. (Hereinafter "OPPR Guidebook")

institution and who is not part of the immediate family of a person who is affiliated with the institution." While the additional four members of the IRB may be affiliated with the institution, the regulations strive to establish a degree of objectivity and balance in the review of research proposals.

As noted, some research falls outside the scope of the federal regulations. Members of the Working Group were not in agreement about the merit of requiring IRB approval for all research. Preliminary studies caution that IRBs are overextended, and the qualifications of members are varied.[26] Some members of the Working Group believed that the extension of federal regulations stands to place additional burdens on IRBs and could dilute their current work. There are also concerns that IRBs are not currently composed to have the requisite experience to judge privacy concerns in research.

Members of the Working Group agreed that an evaluation of the existing IRB system was beyond the scope of its mission. Concerns with the current system were significant enough, however, that members were open to using an alternate review process in situations where IRB approval is not currently required, if it could offer the same potential benefits of the IRB system. Merits of the IRB system, that may or may not be replicable, include:

- a common and independent set of standards;
- requirements for committee composition;
- publicly available decisions; and
- accountability and oversight.

Again, the Working Group agreed not to assess current requirements for IRB approval. Where IRB approval is not currently required, however, a health care organization should have the option to either: 1) obtain IRB approval or 2) use an alternate process that provides an equivalent level of review and accountability.

Standard: Need for Uniformity

Much health-related research that uses personally identifiable health information is conducted with informed consent. However, for some research, it may not be practical to obtain informed consent. In other cases, the project requires full participation—allowing people to refuse participation could bias the results. The Working Group agreed that it was important to provide a mechanism to waive informed consent requirements for some research, as is currently provided under the IRB system. However, as is the case with IRBs, a waiver of informed consent should only be granted if such a determination is made through an objective and balanced process.

---

[26] United States General Accounting Office, *Scientific Research: Continued Vigilance Critical to Protecting Human Subjects,* GAO/HEHS-96-72, (Mar. 8, 1996) and Health and Human Services Inspector General, "Institutional Review Boards: A Time for Reform," OEI-01-97-00193 (June 1998). There are also three companion reports to the HHS report, released simultaneously, entittled "IRB's: Their Role in Reviewing Approved Research," "IRB's: Promising Approaches," and "IRB's: The Emergence of Independent Boards."

Principle #8

Research

Most importantly, there should be uniformity in decisions about when, and under what circumstances, to grant a waiver of informed consent. The *confidentiality* standards articulated in the current federal regulations should serve as the standards for all research—regardless of the body reviewing the proposal. As these standards are revised, they should be incorporated into the policies of the bodies reviewing research proposals.

Regulations governing federally funded research projects require the "informed consent" of "human subjects" participating in a research activity. In evaluating whether to approve a research project that intends to use identifiable data without first obtaining the informed consent of the patient, the IRB must weigh the potential risks to the individual against the "anticipated benefits to the individual or society."[27]

In most circumstances, it is assumed that the researcher will obtain the informed consent of the research participants. The Common Rule, however, allows for exceptions to the informed consent process: some research is exempt from IRB approval, some research is subject to expedited review, and some research is subject to review by the full IRB.

Exempt research: The regulations list many kinds of research that are not subject to IRB review. Of particular note is research that only involves "the collection or study of existing data, documents, records, pathological specimens, or diagnostic specimens, if these sources are publicly available or if the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects."

Expedited review: Under an expedited review, the research project may be approved by a single member of the committee. Types of research that may undergo expedited review are periodically updated by the Secretary of Health and Human Services. Overall, to be eligible for expedited review, the research must (1) involve no more than "minimal risk"[28] or (2) or involve only "minor changes in previously approved research during the period (of one year or less) for which approval is authorized."

In addition to these exceptions, an IRB may alter or waive the consent requirements if the IRB finds that:

> " (1) the research involves no more than minimal risk to the subjects;
> (2) the waiver or alteration will not adversely affect the rights and welfare of the subjects;
> (3) the research could not practicably be carried out without the waiver or the alteration; and
> (4) whenever appropriate, the subjects will be provided with additional pertinent information after participation."

---

[27] OPRR Guidebook at 5-8.

[28] Minimal risk is defined as "the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examination or tests."

The Common Rule, as written, may not provide adequate privacy protections or appropriately address research using databases and archival records.[29] Overall, the current federal regulations are written primarily with an eye toward interventional research studies, such as clinical trials. There is less guidance for research that uses information that identifies individuals, but does not *physically* involve the patient in the research. A review of existing IRB confidentiality standards is currently underway by both HHS and the National Bioethics Advisory Council (NBAC).[30]

The rapid advances in research require some flexibility in standards with regard to confidentiality and research. It is important, however, that there be uniformity in terms of when, and under what circumstances, informed consent requirements can be waived. Whether research is reviewed by an IRB or through an alternate review process it should be held to the same standard. As the standard is revised, pursuant to public comment, it should be applied across the board.

Principle #9

HEALTH CARE ORGANIZATIONS SHOULD NOT DISCLOSE PERSONALLY IDENTIFIABLE HEALTH INFORMATION TO LAW ENFORCEMENT OFFICIALS, ABSENT COMPULSORY LEGAL PROCESS, SUCH AS A WARRANT OR COURT ORDER.

As a general rule, federal privacy laws require that some form of compulsory legal process, based on a standard of proof, be presented in order to disclose to law enforcement officers.[31] Law enforcement access to health information should be held to similar standards.

However, government officials may have legally authorized access to personally identifiable health information to engage in oversight and enforcement of law. In these instances—where compulsory legal process may not be required— information obtained for oversight purposes may not be used against an individual patient in an action unrelated to the oversight nor can the information be re-disclosed, including to another law enforcement agency, except in conformance with the privacy protections that have attached to the data.

Where access has been granted, law enforcement officials should be required to implement appropriate safeguards. In addition to the

---

[29] A recent report published by the General Accounting Office concluded that "[w]hile many organizations have in place IRB review procedures, recent studies pointed to weaknesses in the IRB system, as well as the provisions of the Common Rule itself, suggest that IRB reviews do not ensure the confidentiality of medical information used in research." United States General Accounting Office, *Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections is Limited* (Washington, D.C.: 1999) at 12.

[30] Information and draft reports of the National Bioethics Commission are available on-line at http://bioethics.gov/cgi-bin/bioeth_counter.pl.

[31] See, for example, Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681; Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401; Privacy Protection Act of 1980, 42 U.S.C. § 2000aa; Cable Communications Policy Act of 1984, 47 U.S.C. § 551; Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2703 (a); and Video Privacy Protection Act of 1988, 18 U.S.C. § 2710.

safeguards required for all data-holders (see Principle #5), every effort should be made to prevent information that may identify individuals from entering a public record.

Principle #10

HEALTH PRIVACY PROTECTIONS SHOULD BE IMPLEMENTED IN SUCH A WAY AS TO ENHANCE EXISTING LAWS PROHIBITING DISCRIMINATION.

Patients are understandably concerned that some of their health information can be used in ways to discriminate against them. While this report does not take up the larger issue of discrimination, there is a relationship between privacy protections, and the enforcement of anti-discrimination laws. Privacy protections can reduce the probability that discrimination might happen. For instance, limits on an employer's access to an employee's medical information may limit the employer's opportunity to misuse the information under existing anti-discrimination laws. In this way, privacy may be the first line of defense against discrimination.

The Working Group agreed that privacy policies should be developed and implemented in such a way as to enhance already existing anti-discrimination protections guaranteed by law. At the same time, privacy protections should not be implemented in such a fashion as to effectively create new policies on related issues. Where organizations are engaged in a legally authorized activity, they should have access to patient information, subject to the specified requirements. At the same time, privacy policies should close loopholes and fill in gaps in existing laws, consistent with the overall anti-discrimination policies already fashioned.

Currently, there are state and federal laws that prohibit discrimination on the basis of personally identifiable health information in areas such as employment and insurance underwriting. Also, a number of states have laws prohibiting genetic discrimination. In these areas, appropriate limits on the use of identifiable data may serve to enhance these anti-discrimination laws.

Employer Use of Health Information

Employers use health information for a variety of purposes including employee assistance programs, worker's compensation, on-site delivery of care, and for management of health care benefits.[32] An

[32] Employer use of medical information was taken up in a 1995 court case. In *Doe v. SEPTA*, a federal court found that an employee's privacy interest in shielding his personal health information from his self-insured employers was less compelling than the employer's interest in overseeing its health care plan. A Rite-Aid drug store in Pennsylvania provided to the *Southeastern Pennsylvania Transportation Authority (SEPTA)* information about the prescription drugs being taken by SEPTA's employees. The stated purpose of the disclosure was to allow the state to monitor the costs of its prescription drug program. However, in disclosing to SEPTA authorities that one of its employees was receiving AZT, Rite-Aid in effect disclosed the employee's HIV status. Prior to the disclosure, Doe's employers had assured him that although they were self-insured, no information regarding his prescription drugs or HIV status would be disclosed outside of the Medical Department. The court found no privacy violation stemming from this disclosure since Doe could not prove actual damages and the employer was deemed to have a legitimate interest in knowing the details of how its employees used the health plan. *Doe v. Southeastern Pennsylvania Transportation Authority (SEPTA)*, 72 F.3d 1133 (1995).

employer, for example, may be required to provide "reasonable accommodation" for a disability under the Americans with Disabilities Act.[33] In providing the accommodation the employer may obtain sensitive employee health information. It is not the intent of the Working Group to interfere with the operation of these duties.

There is concern, however, that employer access to health information for these purposes opens the door for employers to use the information for other purposes. Limitations on employer access to, and use of, employee medical data should: 1) not interfere with provisions of the Americans with Disabilities Act (ADA) requiring employers to make reasonable accommodations for people with disabilities; and 2) should close the loop that currently allows employers access to, and use of, employee data in ways not required under the ADA. In many ways, privacy is the first line of defense against discrimination, shielding from employers sensitive employee data that is unrelated to their ability to perform a particular job.

Principle #11

Strong and effective remedies for violations of privacy protections should be established.

To be truly effective, health privacy policies must be buttressed by a set of comprehensive and strong remedies for violation of the policies. It is important that remedies be available for internal and external violations of confidentiality. Unauthorized access within an entity, for example, can be as harmful as disclosure to an outside entity.

Health care organizations should establish appropriate employee training, sanctions, and disciplinary measures for employees and contractors who violate confidentiality policies. Such measures may take into consideration intentional and unintentional actions.

[33] For more information on employer responsibilities under the ADA, see Chai Feldblum, "Medical Examinations and Inquiries Under the Americans with Disabilities Act: A View from the Inside," 64 *Temple Law Review* 521 (1991).

Definitions

Anonymous health information: Information that contains details about a person's medical condition or treatment but the identity of the person cannot be identified.[34]

Disclosure: Sharing of patient information outside an entity. Agents and contractors are considered within an entity (see use).

Health care organizations: A health care organization is any entity that collects, uses, or has access to patient information. The term includes, but is not limited to, health care providers, health plans, public health authorities, employers, life insurers, schools and universities, and health care clearinghouses.

Health information: The term health information means any information, whether oral or recorded in any form or medium, that—(A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.[35]

Non-identifiable health information: Health information from which personal identifiers have been removed, masked, encrypted or otherwise concealed, such that the information can not reasonably be expected to identify individual patients.

Personally identifiable health information: Health information that contains information such that an individual person can be identified as the subject of that information.

Use: Access or sharing of information within an entity, including to an agent or contractor of an entity.

---

[34] Adapted from Latanya Sweeney, "Weaving Technology and Policy Together to Maintain Confidentiality," 25 *Journal of Law, Medicine, & Ethics* 98 (1997).

[35] Health Insurance Portability and Accountability Act of 1996, P.L. 104-191. Also known as Kassebaum- Kennedy.

APPENDIX A: RESOURCES

Randolph C. Barrows, Jr. and Paul D. Clayton, "Privacy, Confidentiality, and Electronic Medical Records," 3 *Journal of the American Medical Informatics Association* 139 (1996).

Paul Clayton, "Technical Measures for Protecting the Confidentiality of Computer-based Health Records," *Protecting the Confidentiality of Patient Information in a Rapidly Changing Health Care System: Summary of a National Conference*, Appendix D (Health Systems Research, Inc. eds., 1998). The conference was sponsored by the Robert Wood Johnson Foundation, held January 14, 1998 in Washington, D.C.

Janlori Goldman and Deirdre Mulligan, Foundation for Health Care Quality, *Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality* (Washington: 1996).

Janlori Goldman and Zoe Hudson, *Promoting Health/Protecting Privacy: A Primer* (California: 1999). Prepared for the California HealthCare Foundation and Consumers Union.

Janlori Goldman, "Protecting Privacy to Improve Health Care," 17 *Health Affairs* 47 (November-December 1998).

Janlori Goldman, "Privacy and Health Information: A Legal Framework," *Protecting the Confidentiality of Patient Information in a Rapidly Changing Health Care System: Summary of a National Conference*, Appendix E (Health Systems Research, Inc. eds., 1998). The conference was sponsored by the Robert Wood Johnson Foundation, held January 14, 1998 in Washington, D.C.

Lawrence Gostin, "Health Information Privacy," 80 *Cornell Law Review* 451 (1995).

Lawrence Gostin et al, *Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization, Final Report Presented to: The U.S. Centers for Disease Control and Prevention; The Council of State and Territorial Epidemiologists; The Task Force for Child Survival and Development Carter Presidential Center* (1997). The report is available at (http://www.epic.org/privacy/medical/cdc_survey.html)

Lawrence Gostin et al, "The Public Health Information Infrastructure: A National Review of the Law on Health Information Privacy," *Journal of the American Medical Association* 391 (June 26, 1996).

Institute of Medicine, *The Computer-Based Patient Record: An Essential Technology for Health Care* (Washington DC: National Academy Press, 1997). The report is available at http://www.nap.edu/readingroom/.

Institute of Medicine, Committee on Regional Health Data Networks, *Health Data in the Information Age* (Washington DC: National Academy Press, 1994). The report is available at http://www.nap.edu/readingroom/.

International Society for Pharmacoepidemiology, *Data Privacy, Medical Record Confidentiality, and Research in the Interest of Public Health* (Washington DC: September 1997). The report can also be found at http://www.pharmacoepi.org.

Shannah Koss, "White Paper - Health Insurance Portability and Accountability Act: Security Standards; Implications for the Healthcare Industry," IBM White Paper (1998). The paper is available at http://www.solutions.ibm.com/healthcare/solution/whitep1.html.

Bernard Lo, "Confidentiality of Patient Information in a Changing Health Care System" in *Protecting the Confidentiality of Patient Information in a Rapidly Changing Health Care System: Summary of a National Conference*, Appendix F (Health Systems Research, Inc. eds., 1998). The conference was sponsored by the Robert Wood Johnson Foundation, held January 14, 1998 in Washington, D.C.

Bernard Lo, *Resolving Ethical Dilemmas: A Guide for Clinicians* (Baltimore, Maryland: Williams and Wilkins, 1995).

William Lowrance, U.S. Department of Health and Human Services, *Privacy and Health Research: A Report to the U.S. Secretary of Health and Human Services* (May 1997). The report is available at http://aspe.os.dhhs.gov/datacncl/PHR.htm.

National Committee for Quality Assurance and the Joint Commission on Accreditation of Healthcare Organizations, *Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment* (Washington DC: 1998). The report is available at http://www.ncqa.org/confide/tablcont.htm.

National Committee on Vital and Health Statistics, *Health Privacy and Confidentiality Recommendations* (Washington DC: June 25, 1997). Full text is available at http://aspe.os.dhhs.gov/ncvhs/privrecs.htm.

National Research Council, *For the Record: Protecting Electronic Health Information* (Washington DC: National Academy Press, 1997). Full text is available at http://www.nap.edu/readingroom/.

Office of Technology Assessment, United States Congress, *Protecting Privacy in Computerized Medical Information* (September 1993). The report is available at http://www.wws.princeton.edu/~ota/ns20/alpha_f.html.

The President's Advisory Commission on Consumer Protection and Quality in the Health Care Industry, *Quality First: Better Health Care for All Americans* (1998). See Appendix A: Consumer Bill of Rights and Responsibilities, pp. A57-A60 for "Confidentiality of Health Information." To order, call 800-732-8200; ISBN 0-16-049533-4.

William Roach and the Aspen Health Law and Compliance Center, *Medical Records and the Law*. (Gaithersburg, Maryland: Aspen

Publishers, 1998).

Latanya Sweeney, "Controlling Inference and Protecting Privacy by Constructing an Anonymous Data System" (Carnegie Mellon University: Unpublished paper, November 1998).

Latanya Sweeney, "Weaving Technology and Policy Together to Maintain Confidentiality," 25 *Journal of Law, Medicine, & Ethics* 98 (1997).

United States Department of Health and Human Services, *Confidentiality of Individually-Identifiable Health Information, Recommendations Submitted to Congress* (September 1997). Full text is available at http://aspe.os.dhhs.gov/admnsimp/pvcrec0.htm.

United States Department of Health and Human Services, *Administrative Simplification Home Page*. Includes proposed Rules and Comments, http://aspe.os.dhhs.gov/admnsimp.

United States Department of Labor, *Genetic Information and the Workplace* (January 20, 1998). The report is available at http://www.dol.gov/dol/_sec/public/media/reports/genetics.htm.

United States General Accounting Office, *Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections Limited* (GAO/HEHS-99-55, February 1999).

APPENDIX B: MEMBER BIOGRAPHIES

Paul Clayton

Paul D. Clayton, a native of Salt Lake City, Utah, received his Ph.D. in physics from the University of Arizona in 1973. He then developed and implemented information systems in cardiology, radiology and surgery at LDS Hospital and the University of Utah. He joined Columbia in 1987 as director of the Center for Medical Informatics and professor of medical informatics. He became chairman of the newly created Department of Medical Informatics in 1994. When Dr. Clayton joined Columbia, he led efforts to build an integrated information system for the medical center, an effort supported by an Integrated Advanced Information Management System grant from the National Library of Medicine. He was also active in creating an advanced clinical information system with decision-making capability now widely used at CPMC. Dr. Clayton is president of the American Medical Informatics Association and an elected fellow of the American College of Medical Informatics and the Institute of Medicine. Dr. Clayton chaired a National Research Council committee addressing issues of confidentiality of health records on the national information infrastructure.

Jeff Crowley

Jeff Crowley is the deputy executive director for programs of the National Association of People with AIDS (NAPWA). Mr. Crowley oversees NAPWA's education department and the community development and training department. He is a co-chair of the Health Task Force of the Consortium for Citizens with Disabilities and has convened the Coalition for Emergency Action on Medicaid Funding. Mr. Crowley is also a member of the National Academy for State Health Policy's Working Group on Medicaid Managed Care for People with AIDS. He received his bachelor of arts from Kalamazoo College in Michigan where he majored in chemistry and earned a master's in public health from Johns Hopkins University.

John Glaser

John Glaser is vice-president and chief information officer, Partners HealthCare System, Inc., an integrated delivery system founded by the Brigham and Women's Hospital and Massachusetts General Hospital. Previously, he was vice-president, information systems at Brigham and Women's Hospital.

He was founding chairman, College of Healthcare Information Management Executives (CHIME) and past-president, Healthcare Information and Management Systems Society (HIMSS). He is the 1994 recipient of the John Gall award for Healthcare CIO of the year.

Prior to Brigham and Women's Hospital, Dr. Glaser managed the Healthcare Information Systems consulting practice at Arthur D. Little. He holds a Ph.D. in Healthcare Information Systems from the University of Minnesota.

Nan Hunter

Nan D. Hunter is a professor of law at Brooklyn Law School. In the spring of 1998, she was a visiting professor of law at Harvard Law School. In 1986, prior to entering teaching, she founded and became the first director of the ACLU AIDS Project. From 1993 to 1996, she was deputy general counsel at the U.S. Department of Health and Human Services. In 1997, she was appointed to the President's Advisory Commission on Consumer Protection and Quality in the Health Care Industry. She is a Fellow of the New York Academy of Medicine. She is the author of numerous articles in the area of constitutional law, civil rights, and health law.

Shannah Koss

Shannah Koss is the health care security and government programs executive at IBM Corporation. She is the marketing manager for the government health-care segment and responsible for positioning IBM's health-care IT capabilities in response to changes in the legal requirements for the health-care market. Ms. Koss is currently leading the establishment of IBM's Healthcare Security Practice. Prior to joining IBM, Ms. Koss was the manager for the Federal Office of Management and Budget overseeing health care programs and federal health care information requirements. She was the co-chair of the Information Systems Working Group in the Clinton Administration Health Care Task Force. She has a bachelor's degree from the University of Chicago and a master's from the John F. Kennedy School of Government at Harvard University.

Chris Koyanagi

Chris Koyanagi is policy director for the Judge David L. Bazelon Center for Mental Health Law in Washington, D.C. The Bazelon Center is a legal advocacy organization concerned with the rights of children and adults with mental impairments. Chris is responsible for the legislative and policy advocacy agenda of the Bazelon Center. The Center's priorities are to ensure community membership for persons with mental illness, including access to community based services and protection of individual rights to choice. Ms. Koyanagi works on policy issues with respect to financing mental health services, particularly through Medicaid, the use of advance directives for mental health care, consumer rights under public sector managed care plans, access to housing, income support, education, rehabilitation and other essential community services for adults and children with mental disorders.

Chris has nearly 30 years of Washington experience working on human services issues and in addition to her work at the Bazelon Center, serves on several mental health policy advisory committees and has authored numerous articles and other publications on mental health policy.

Bernard Lo, Chair

Bernard Lo, M.D., is professor of medicine and director of the Program in Medical Ethics at the University of California San Francisco. He directs the national coordinating office of the Initiative to Strengthen the Patient-Provider Relationship in a Changing Health Care Environment, which is funded by the Robert Wood Johnson Foundation. He chairs the End of Life Committee convened by the American College of Physicians, which will develop recommendations for clinical care near the end of life.

Dr. Lo is a member of the National Bioethics Advisory Commission, which issued a report in June 1997 on cloning of human beings. He is also a member of the Data Safety Monitoring Board for the AIDS Clinical Trials Group at the National Institute of Allergy and Infectious Diseases. He is a member of the Institute of Medicine and serves on its Board of Health Sciences Policy. He served on the White House Task Force on Health Care Reform and the National Institutes of Health advisory board on human embryo research.

Dr. Lo has written over one hundred articles in peer-reviewed medical journals, on such issues as decisions about life-sustaining interventions, decision-making for incompetent patients, physician-assisted suicide, and ethical issues regarding HIV infection. He is the author of *Resolving Ethical Dilemmas: A Guide for Clinicians*, a comprehensive analysis of ethical dilemmas in adult clinical medicine. He is also a practicing general internist and teaches clinical medicine to residents and medical students.

John T. Nielsen

John T. Nielsen is currently Senior Counsel and Director of Government Relations for Intermountain Health Care, Salt Lake City, Utah. In that capacity he is responsible for government relations and public policy in the states of Utah, Idaho, Wyoming and also in Washington, D.C. Mr. Nielsen is a frequent witness at both the state and national level with issues involving health care, health insurance and medical records privacy and confidentiality. He also serves as a member or chairs numerous state boards and task forces dealing with health care and insurance-related issues. Mr. Nielsen is also of-counsel in the Salt Lake City firm of Van Cott, Bagley, Cornwall & McCarthy. As a senior partner in that law firm, he practiced in the area of government and legislative relations, administrative and regulatory matters, and civil and criminal litigation.

Mr. Nielsen began his career in government in 1970 as an Assistant Salt Lake City Attorney. In 1973 he became legal advisor to the Salt Lake City Police Department. Mr. Nielsen joined the office of the Salt Lake County Attorney as a felony prosecutor in 1975. He was the Chief Deputy of the Justice Division of the Salt Lake County Attorney's Office from 1979 to 1985. Mr. Nielsen was appointed Utah Commissioner of Public Safety in March 1985 serving until 1989.

He is a member of the Utah State Bar, the American Bar Association, and the American Academy of Health Care Attorneys. He also chairs or serves as a member of various government councils and

commissions, and is active in civic and church affairs. Mr. Nielsen is a native of Salt Lake City. He graduated from the University of Utah with a B.S. in Business Management in 1967 and from the University of Utah College of Law with his Juris Doctorate in 1969. He is married and has four daughters.

Linda K. Shelton

Linda Shelton is assistant vice president for product development for the National Committee for Quality Assurance (NCQA). Ms. Shelton led the team that developed Accreditation '99, which for the first time integrates HEDIS and Accreditation, and is now leading NCQA's efforts to develop new accreditation products for PPOs and other organizations. She has also developed NCQA Accreditation's public reports, conducted over 35 accreditation surveys and served as faculty for NCQA conferences. She has a master's degree in health care administration from George Washington University.

Margaret Anne VanAmringe

Ms. VanAmringe is vice-president for external relations at the Joint Commission on Accreditation of Healthcare Organizations. She is responsible for developing new strategic opportunities for the Joint Commission, especially in the area of managed care. She also directs their Washington Office, which is concerned with developing new directions for the Commission in response to federal and private sector initiatives. She works on policy issues involving outcomes and other performance measurement of health care organizations, health care privacy, quality of care oversight, and health care policy.

Just prior to taking a position at the Joint Commission, Ms. VanAmringe was director, Center for Research Dissemination and liaison at the Agency for Health Care Policy and Research in the U.S. Public Health Service. As director, she established programs to communicate health services research findings, including clinical practice guideline and outcomes research information, to a wide array of professional and public audiences. At AHCPR she developed the first extramural grant program to investigate the best methods of encouraging clinicians to change their practices based on new medical evidence. Ms. VanAmringe also initiated AHCPR's first health information dissemination program to bring practical health services research information into the hands of consumers and their families.

From 1989 to mid 1990, Ms. VanAmringe was a legislative fellow in the Office of Senator George Mitchell (D-Me.) where she drafted health legislation in areas such as health services research, biomedical research and long-term care.

From 1988 to 1989, she held several positions in the Immediate Office of the Secretary, Department of Health and Human Services, including senior advisor to the chief of staff. During these times, she provided advice on the full range of social and health policy issues. Before joining the Secretary's staff, she spent eight years working in the Health Care Financing Administration where she directed their Office of Survey and Certification, the component responsible for

assuring that health care facilities reimbursed by Medicare/Medicaid meet quality of care and safety standards.

Ms. VanAmringe is on the board of Health Commons Institute, a private not-for-profit organization whose mission is to improve Health care outcome through shared decision making between clinicians and patients using computer-assisted methodologies and databases. She received her masters degree from the Johns Hopkins School of Hygiene and Public Health.

APPENDIX C: STAFF BIOGRAPHIES

Janlori Goldman

Janlori Goldman directs the Health Privacy Project at Georgetown University's Institute for Health Care Research and Policy. Ms. Goldman created the Project in December 1997. The Project is dedicated to ensuring that peoples' privacy is safeguarded in the health care environment. In 1997, Ms. Goldman was a Visiting Scholar at Georgetown University Law Center. In 1994, Ms. Goldman co-founded the Center for Democracy and Technology, a non-profit civil liberties organization committed to preserving free speech and privacy on the Internet. Ms. Goldman also worked at the Electronic Frontier Foundation in 1994. From 1986 to 1994, Ms. Goldman was the staff attorney and director of the Privacy and Technology Project of the American Civil Liberties Union (ACLU). While at the ACLU, Ms. Goldman led the effort to enact the Video Privacy Protection Act and led efforts to protect peoples' health, credit and financial information and personal information held by the government. She was the legislative director of the Minnesota affiliate of the ACLU from 1984-86.

Ms. Goldman has testified frequently before the U.S. Congress and served on numerous commissions and advisory boards. Her publications include "A Federal Right of Information Privacy," co-authored with Jerry Berman, and included as a chapter in *Computers, Ethics, and Social Values*, ed. Helen Nissenbaum, Prentice Hall, 1995; *Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality*, co-authored with Deirdre Mulligan, Foundation for Health Care Quality, 1996; "Protecting Privacy to Improve Health Care," *Health Affairs*, Nov/Dec 1998; and most recently, *Promoting Health/Protecting Privacy: A Primer*, co- authored with Zoe Hudson, California HealthCare Foundation and Consumers Union, 1999.

Zoe Hudson

Zoe Hudson is a policy analyst with the Health Privacy Project at Georgetown University's Institute for Health Care Research and Policy. The Project is dedicated to ensuring that peoples' privacy is safeguarded in the health care environment. Ms. Hudson joined the Project in March 1998 and her responsibilities include staffing the Health Privacy Working Group, and developing a comprehensive state survey of health privacy laws. Ms. Hudson co-authored with Janlori Goldman *Promoting Health/Protecting Privacy: A Primer* for the California HealthCare Foundation and Consumers Union. In addition, Ms. Hudson has written testimony for the U.S. Congress. Before coming to the Health Privacy Project, Ms. Hudson was the program and policy director for Parents, Families and Friends of Lesbians and Gays (PFLAG), a national, grassroots organization. She received her bachelor of arts from Grinnell College in Iowa.