PHOTOCOPY
PRESERVATION

PRIVACY

HEALTH PRIVACY PROJECT

INSTITUTE FOR HEALTH CARE RESEARCH AND POLICY
GEORGETOWN UNIVERSITY

File Privacy

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

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.

Best Principles for Health Privacy

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

Executive Summary

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.