MMWR™

Morbidity and Mortality Weekly Report

Early Release April 11, 2003 / Vol. 52

HIPAA Privacy Rule and Public Health

Guidance from CDC and the U.S. Department of Health and Human Services

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR DISEASE CONTROL AND PREVENTION

The *MMWR* series of publications is published by the Epidemiology Program Office, Centers for Disease Control and Prevention (CDC), U.S. Department of Health and Human Services, Atlanta, GA 30333.

SUGGESTED CITATION

Centers for Disease Control and Prevention. HIPAA Privacy Rule and public health: guidance from CDC and the U.S. Department of Health and Human Services. MMWR 2003;52(Early Release):[inclusive page numbers].

Centers for Disease Control and Prevention

Julie L. Gerberding, M.D., M.P.H.
Director

David W. Fleming, M.D.
Deputy Director for Public Health Science

Dixie E. Snider, Jr., M.D., M.P.H.
Associate Director for Science

Epidemiology Program Office

Stephen B. Thacker, M.D., M.Sc.
Director

Office of Scientific and Health Communications

John W. Ward, M.D.
Director
Editor, MMWR *Series*

Suzanne M. Hewitt, M.P.A.
Managing Editor, MMWR *Series*

C. Kay Smith-Akin, M.Ed.
Lead Technical Writer/Editor

Douglas W. Weatherwax
Project Editor

Beverly J. Holland
Lead Visual Information Specialist

Malbea A. Heilman
Visual Information Specialist

Quang M. Doan
Erica R. Shaver
Information Technology Specialists

CONTENTS

Introduction 1
Impact on Public Health 2
Overview of the Privacy Rule 3
Who Is Covered 3
Types of Health Information 3
What is Required 4
The Privacy Rule and Public Health 6
Disclosures for Public Health Purposes 8
Requirements for Covered Entities 8
The Privacy Rule and Public Health Research 10
Research Versus Practice 10
The Privacy Rule and Other Laws 10
Online Resources 11
Federal Government Resources 11
State Government Resources 11
Associations, Nonprofit Organizations, and Academic Resources 12
Acknowledgments 12
References 12
Appendix A 13
Appendix B 19

HIPAA Privacy Rule and Public Health

Guidance from CDC and the U.S. Department of Health and Human Services*

Summary

New national health information privacy standards have been issued by the U.S. Department of Health and Human Services (DHHS), pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The new regulations provide protection for the privacy of certain individually identifiable health data, referred to as protected health information (PHI). Balancing the protection of individual health information with the need to protect public health, the Privacy Rule expressly permits disclosures without individual authorization to public health authorities authorized by law to collect or receive the information for the purpose of preventing or controlling disease, injury, or disability, including but not limited to public health surveillance, investigation, and intervention.

Public health practice often requires the acquisition, use, and exchange of PHI to perform public health activities (e.g., public health surveillance, program evaluation, terrorism preparedness, outbreak investigations, direct health services, and public health research). Such information enables public health authorities to implement mandated activities (e.g., identifying, monitoring, and responding to death, disease, and disability among populations) and accomplish public health objectives. Public health authorities have a long history of respecting the confidentiality of PHI, and the majority of states as well as the federal government have laws that govern the use of, and serve to protect, identifiable information collected by public health authorities.

The purpose of this report is to help public health agencies and others understand and interpret their responsibilities under the Privacy Rule. Elsewhere, comprehensive DHHS guidance is located at the HIPAA website of the Office for Civil Rights (http://www.hhs.gov/ocr/hipaa/).

Introduction

The shift of medical records from paper to electronic formats has increased the potential for individuals to access, use, and disclose sensitive personal health data. Although protecting individual privacy is a long-standing tradition among health-care providers and public health practitioners in the United States, previous legal protections at the federal, tribal, state, and local levels were inconsistent and inadequate. A patchwork of laws provided narrow privacy protections for selected health data and certain keepers of that data (*1*).

The U.S. Department of Health and Human Services (DHHS) has addressed these concerns with new privacy standards that set a national minimum of basic protections, while balancing individual needs with those of society. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was adopted to ensure health insurance coverage after leaving an employer and also to provide standards for facilitating health-care–related electronic transactions. To improve the efficiency and effectiveness of the health-care system, HIPAA included administrative simplification provisions that required DHHS to adopt national standards for electronic health-care transactions (*2*). At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated adoption of federal privacy protections for certain individually identifiable health information.

The HIPAA Privacy Rule (Standards for Privacy of Individually Identifiable Health Information) (*3*) provides the first national standards for protecting the privacy of health information. The Privacy Rule regulates how certain entities, called covered entities, use and disclose certain individually identifiable health information, called protected health information (PHI). PHI is individually identifiable health information that is transmitted or maintained in any form or medium (e.g., electronic, paper, or oral), but excludes certain educational records and employment records. Among other provisions, the Privacy Rule

- gives patients more control over their health information;
- sets boundaries on the use and release of health records;
- establishes appropriate safeguards that the majority of health-care providers and others must achieve to protect the privacy of health information;

* Prepared by CDC staff, in consultation with the Office of the General Counsel, the Office for Civil Rights, other offices and agencies within the U.S. Department of Health and Human Services, Washington, D.C., and health privacy specialists.

The material in this report originated in the Epidemiology Program Office, Stephen B. Thacker, M.D., M.Sc., Director.

- holds violators accountable with civil and criminal penalties that can be imposed if they violate patients' privacy rights;
- strikes a balance when public health responsibilities support disclosure of certain forms of data;
- enables patients to make informed choices based on how individual health information may be used;
- enables patients to find out how their information may be used and what disclosures of their information have been made;
- generally limits release of information to the minimum reasonably needed for the purpose of the disclosure;
- generally gives patients the right to obtain a copy of their own health records and request corrections; and
- empowers individuals to control certain uses and disclosures of their health information.

The deadline to comply with the Privacy Rule is April 14, 2003, for the majority of the three types of covered entities specified by the rule [45 CFR § 160.102]. The covered entities are

- health plans,
- health-care clearinghouses, and
- health-care providers who transmit health information in electronic form in connection with certain transactions.

At DHHS, the Office for Civil Rights (OCR) has oversight and enforcement responsibilities for the Privacy Rule. Comprehensive guidance and OCR answers to hundreds of questions are available at http://www.hhs.gov/ocr/hipaa (*4*).

Impact on Public Health

Public health practice and research, including such traditional public health activities as program operations, public health surveillance, program evaluation, terrorism preparedness, outbreak investigations, direct health services, and public health research, use PHI to identify, monitor, and respond to disease, death, and disability among populations. Public health authorities have a long history of protecting and preserving the confidentiality of individually identifiable health information. They also recognize the importance of protecting individual privacy and respecting individual dignity to maintaining the quality and integrity of health data. CDC and others have worked to consistently strengthen federal and state public health information privacy practices and legal protections (*5*).

DHHS recognized the importance of sharing PHI to accomplish essential public health objectives and to meet certain other societal needs (e.g., administration of justice and law enforcement). Therefore, the Privacy Rule expressly permits PHI to be shared for specified public health purposes. For example, covered entities may disclose PHI, without individual authorization, to a public health authority legally authorized to collect or receive the information for the purpose of preventing or controlling disease, injury, or disability [45 CFR § 164.512(b)] (Box 1). Further, the Privacy Rule permits covered entities to make disclosures that are required by other laws, including laws that require disclosures for public health purposes.

Thus, the Privacy Rule provides for the continued functioning of the U.S public health system. Covered entities should become fully aware of the scope of permissible disclosures for public health activities as well as state and local reporting laws and regulations. Moreover, a public health authority may also

BOX 1. Protected health information (PHI) disclosures by covered entities for public health activities requiring no authorization under the Privacy Rule

Without individual authorization, a covered entity may disclose PHI to a public health authority* that is legally authorized to collect or receive the information for the purposes of preventing or controlling disease, injury, or disability including, but not limited to

- reporting of disease, injury, and vital events (e.g., birth or death); and
- conducting public health surveillance, investigations, and interventions.

PHI may also be disclosed without individual authorization to

- report child abuse or neglect to a public health or other government authority legally authorized to receive such reports;
- a person subject to jurisdiction of the Food and Drug Administration (FDA) concerning the quality, safety, or effectiveness of an FDA-related product or activity for which that person has responsibility;
- a person who may have been exposed to a communicable disease or may be at risk for contracting or spreading a disease or condition, when legally authorized to notify the person as necessary to conduct a public health intervention or investigation; and
- an individual's employer, under certain circumstances and conditions, as needed for the employer to meet the requirements of the Occupational Safety and Health Administration, Mine Safety and Health Administration, or a similar state law.

Source: Adapted from [45 CFR § 164.512(b)].

* Or to an entity working under a grant of authority from a public health authority, or when directed by a public health authority, to a foreign government agency that is acting in collaboration with a public health authority.

be a covered entity. For example, a public health agency that operates a health clinic, providing essential health-care services and performing covered transactions electronically, is a covered entity.

This report provides guidance to public health authorities and their authorized agents, researchers, and health-care providers in interpreting the Privacy Rule as it affects public health. CDC recommends that public health authorities share the information in this report with covered health-care providers and other covered entities and work closely with those entities to ensure implementation of the rule consistent with its intent to protect privacy while permitting authorized public health activities to continue.

Overview of the Privacy Rule

Who Is Covered

The authority of DHHS to issue health-information privacy regulations was limited by Congress in HIPAA to a defined set of covered entities. More complete definitions of these, and other terms, are located elsewhere in this report (Appendix A). Covered entities are as follows:

- Health plans. An individual or group plan that provides, or pays the cost of, medical care that includes the diagnosis, cure, mitigation, treatment, or prevention of disease. Health plans include private entities (e.g., health insurers and managed care organizations) and government organizations (e.g., Medicaid, Medicare, and the Veterans Health Administration).
- Health-care clearinghouses. A public or private entity, including a billing service, repricing company, or community health information system, that processes nonstandard data or transactions received from another entity into standard transactions or data elements, or vice versa.
- Health-care providers. A provider of health-care services and any other person or organization that furnishes, bills, or is paid for health care in the normal course of business. Health-care providers (e.g., physicians, hospitals, and clinics) are covered entities if they transmit health information in electronic form in connection with a transaction for which a HIPAA standard has been adopted by DHHS.

The Privacy Rule also establishes requirements for covered entities with regard to their nonemployee business associates (e.g., lawyers, accountants, billing companies, and other contractors) whose relationship with covered entities requires sharing of PHI. The Privacy Rule allows a covered provider or health plan to disclose PHI to a business associate if satisfactory written assurance is obtained that the business associate will use the information only for the purposes for which it was engaged, will safeguard the information from misuse, and will help the covered entity comply with certain of its duties under the Privacy Rule.

The Privacy Rule does not apply to all persons or entities that regularly use, disclose, or store individually identifiable health information. For example, the Privacy Rule does not cover employers, certain insurers (e.g., auto, life, and worker compensation), or those public agencies that deliver social security or welfare benefits, when functioning solely in these capacities.

Types of Health Information

Protected Health Information

The Privacy Rule protects certain information that covered entities use and disclose. This information is called protected health information (PHI), which is generally individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to 1) the past, present, or future physical or mental health, or condition of an individual; 2) provision of health care to an individual; or 3) payment for the provision of health care to an individual. If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered individually identifiable health information.

De-Identified Information

De-identified data (e.g., aggregate statistical data or data stripped of individual identifiers) require no individual privacy protections and are not covered by the Privacy Rule. De-identifying can be conducted through

- statistical de-identification — a properly qualified statistician using accepted analytic techniques concludes the risk is substantially limited that the information might be used, alone or in combination with other reasonably available information, to identify the subject of the information [45 CFR § 164.514(b)]; or the
- safe-harbor method — a covered entity or its business associate de-identifies information by removing 18 identifiers (Box 2) and the covered entity does not have actual knowledge that the remaining information can be used alone or in combination with other data to identify the subject [45 CFR § 164.514(b)].

In certain instances, working with de-identified data may have limited value to clinical research and other activities. When that is the case, a limited data set may be useful.

BOX 2. Individual identifiers under the Privacy Rule

The following 18 identifiers of a person, or of relatives, employers, or household members of a person must be removed, and the covered entity must not have actual knowledge that the information could be used alone or in combination with other information to identify the individual, for the information to be considered de-identified and not protected health information (PHI):

- names;
- all geographic subdivisions smaller than a state, including county, city, street address, precinct, zip code,* and their equivalent geocodes;
- all elements of dates (except year) directly related to an individual; all ages >89 and all elements of dates (including year) indicative of such age (except for an aggregate into a single category of age >90);
- telephone numbers;
- fax numbers;
- electronic mail addresses;
- Social Security numbers;
- medical record numbers;
- health-plan beneficiary numbers;
- account numbers;
- certificate and license numbers;
- vehicle identifiers and serial numbers, including license plate numbers;
- medical device identifiers and serial numbers;
- Internet universal resource locators (URLs);
- Internet protocol (IP) addresses;
- biometric identifiers including fingerprints and voice prints;
- full-face photographic images and any comparable images; and
- any other unique identifying number, characteristic, or code, except that covered identities may, under certain circumstances, assign a code or other means of record identification that allows de-identified information to be re-identified.

Source: Adapted from [45 CFR § 164.514(b)(2)(i)].

* The first three digits of a zip code are excluded from the PHI list if the geographic unit formed by combining all zip codes with the same first three digits contains >20,000 persons.

BOX 3. Use of limited data sets under the Privacy Rule

The following protected health information (PHI) can be included, without authorization, in a limited data set for public health, research, or health-care operations:

- town or city, state, and zip code; and
- elements of dates related to a person (e.g., years, birth dates, admission dates, discharge dates, and dates of death).

To disclose a limited data set, a covered entity must enter into a data-use agreement with the recipient, which agrees to use or disclose the PHI for limited purposes. Disclosure of a limited data set is not subject to the accounting requirement, but must meet the minimum necessary standards of the Privacy Rule.

Limited Data Sets

Health information in a limited data set is not directly identifiable, but may contain more identifiers than de-identified data that has been stripped of the 18 identifiers [45 CFR § 164.514] (Box 3). A data-use agreement must establish who is permitted to use or receive the limited data set, and provide that the recipient will

- not use or disclose the information other than as permitted by the agreement or as otherwise required by law;
- use appropriate safeguards to prevent uses or disclosures of the information that are inconsistent with the data-use agreement;
- report to the covered entity any use or disclosure of the information, in violation of the agreement, of which it becomes aware;
- ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
- not attempt to re-identify the information or contact the individual.

What is Required

For covered entities using or disclosing PHI, the Privacy Rule establishes a range of health-information privacy requirements and standards that attempt to balance individual privacy interests with the community need to use such data [45 CFR § 164.504]. Among its provisions, the Privacy Rule requires covered entities to

- notify individuals regarding their privacy rights and how their PHI is used or disclosed;
- adopt and implement internal privacy policies and procedures;
- train employees to understand these privacy policies and procedures as appropriate for their functions within the covered entity;

- designate individuals who are responsible for implementing privacy policies and procedures, and who will receive privacy-related complaints;
- establish privacy requirements in contracts with business associates that perform covered functions;
- have in place appropriate administrative, technical, and physical safeguards to protect the privacy of health information; and
- meet obligations with respect to health consumers exercising their rights under the Privacy Rule.

With respect to individuals, they are vested with the following rights:

- Receive access to PHI. Individual rights include inspections of records and the provision for copies of PHI about the individual in a designated record set, for as long as the PHI is maintained in the designated record set, except for psychotherapy notes, information complied for use in civil, criminal, or administrative actions, and PHI maintained by a covered entity subject to the Clinical Laboratory Improvement Amendments of 1988 [42 CFR § 263(a)]. In the majority of cases, covered entities must accommodate a request or provide a process of denial, subject to review [45 CFR § 164.524].
- Request amendments to PHI. Individuals can request that covered entities amend PHI about the individual in a designated record set for as long as the PHI is maintained in a designated record set. If the covered entity agrees to the amendment, it must 1) identify the records affected; 2) append or provide a link to the amendment; 3) inform the individual the amendment has been made; and 4) work with other covered entities or business associates who possess or receive the data to make the amendments [45 CFR § 164.526]. If the covered entity denies this request, the Privacy Rule provides a process for contesting the denial [45 CFR § 164.526].
- Receive adequate notice. With limited exceptions, individuals have the right to receive a notice of the uses and disclosures the covered entity will make of their PHI, their rights under the Privacy Rule, and the covered entity's obligations with respect to that information. In certain cases, notice may be provided electronically. The notice must be in plain language (e.g., "your health information may be shared with public health authorities for public health purposes . . .") and posted where it is likely to be seen by patients [45 CFR § 164.520].
- Receive an accounting of disclosures. Upon request, covered entities are required to provide individuals with an accounting for certain types of disclosures of PHI, although the rule contains certain exceptions, including disclosures with individual authorization, disclosures related to providers' treatment, payment and health-care operations (TPO), and other exceptions. A typical a ccounting includes the name of the person or entity who received the information, date of the disclosure, a brief description of the information disclosed, and a brief e xplanation of the reasons for disclosure or copy of the request [45 CFR § 164.528]. However, requirements for accounting of public health disclosures may vary (see Accounting for Public Health Disclosures).
- Request restrictions. Individuals have the right to request a restriction on certain uses or disclosures of their PHI; however, the covered entity is not obligated to agree to such a request. If the covered entity does agree to a restriction, it must generally abide by the agreement, except for emergency treatment situations. But such an agreement is not effective to prevent certain permitted uses or disclosures [CFR 45 § 164.512].

Required PHI Disclosures

A covered entity is required by the Privacy Rule to disclose PHI in only two instances: 1) when an individual has a right to access an accounting of his or her PHI (see previous paragraph); and 2) when DHHS needs PHI to determine compliance with the Privacy Rule [45 CFR § 164.502(a)(2)]. Certain other uses and disclosures of PHI may be permitted without authorization, but are not required by the Privacy Rule. However, other federal, tribal, state, or local laws may compel disclosure.

Permitted PHI Disclosures Without Authorization

The Privacy Rule permits a covered entity to use and disclose PHI, with certain limits and protections, for TPO activities [45 CFR § 164.506]. Certain other permitted uses and disclosures for which authorization is not required follow. Additional requirements and conditions apply to these disclosures. The Privacy Rule text and OCR guidance should be consulted for a full understanding of the following:

- Required by law. Disclosures of PHI are permitted when required by other laws, whether federal, tribal, state, or local.
- Public health. PHI can be disclosed to public health authorities and their authorized agents for public health purposes including but not limited to public health surveillance, investigations, and interventions.
- Health research. A covered entity can use or disclose PHI for research without authorization under certain conditions, including 1) if it obtains documentation of a waiver from an institutional review board (IRB) or a privacy board, according to a series of considerations; 2) for

activities preparatory to research; and 3) for research on a decedent's information.

- Abuse, neglect, or domestic violence. PHI may be disclosed to report abuse, neglect, or domestic violence under specified circumstances.
- Law enforcement. Covered entities may, under specified conditions, disclose PHI to law enforcement officials pursuant to a court order, subpoena, or other legal order, to help identify and locate a suspect, fugitive, or missing person; to provide information related to a victim of a crime or a death that may have resulted from a crime, or to report a crime.
- Judicial and administrative proceedings. A covered entity may disclose PHI in the course of a judicial or administrative proceeding under specified circumstances.
- Cadaveric organ, eye, or tissue donation purposes. Organ-procurement agencies may use PHI for the purposes of facilitating transplant.
- Oversight. Covered entities may usually disclose PHI to a health oversight agency for oversight activities authorized by law.
- Worker's compensation. The Privacy Rule permits disclosure of work-related health information as authorized by, and to the extent necessary to comply with, workers' compensation programs.

Other Authorized Disclosures

A valid authorization is required for any use or disclosure of PHI that is not required or otherwise permitted without authorization by the Privacy Rule. In general, these authorizations must

- specifically identify the PHI to be used or disclosed;
- provide the names of persons or organizations, or classes of persons or organizations, who will receive, use, or disclose the PHI;
- state the purpose for each request;
- notify individuals of their right to refuse to sign the authorization without negative consequences to treatment, payment, or health plan enrollment or benefit eligibility, except under specific circumstances;
- be signed and dated by the individual or the individual's personal representative;
- be written in plain language;
- include an expiration date or event;
- notify the individual of the right to revoke authorization at any time in writing, and how to exercise that right, and any applicable exceptions to that right under the Privacy Rule; and
- explain the potential for the information to be subject to redisclosure by recipient and no longer protected by the Privacy Rule.

The Privacy Rule and Public Health

The Privacy Rule recognizes 1) the legitimate need for public health authorities and others responsible for ensuring the public's health and safety to have access to PHI to conduct their missions; and 2) the importance of public health reporting by covered entities to identify threats to the public and individuals. Accordingly, the rule 1) permits PHI disclosures without a written patient authorization for specified public health purposes to public health authorities legally authorized to collect and receive the information for such purposes, and 2) permits disclosures that are required by state and local public health or other laws. However, because the Privacy Rule affects the traditional ways PHI is used and exchanged among covered entities (e.g., doctors, hospitals, and health insurers), it can affect public health practice and research in multiple ways. To prevent misconceptions, understanding the Privacy Rule is important for public health practice. Some illustrative examples are presented in this report (Box 4). Also provided are sample letters that might prove useful in clarifying relationships involving public health and the Privacy Rule (Appendix B).

A public health authority is broadly defined as including agencies or authorities of the United States, states, territories, political subdivisions of states or territories, American Indian tribes, or an individual or entity acting under a grant of authority from such agencies and responsible for public health matters as part of an official mandate. Public health authorities include federal public health agencies (e.g., CDC, National Institutes of Health [NIH], Health Resources and Services Administration [HRSA], Substance Abuse and Mental Health Services Administration [SAMHSA], Food and Drug Administration [FDA], or Occupational Safety and Health Administration [OSHA]); tribal health agencies; state public health agencies (e.g., public health departments or divisions, state cancer registries, and vital statistics departments); local public health agencies; and anyone performing public health functions under a grant of authority from a public health agency [45 CFR § 164.501].

Public health agencies often conduct their authorized public health activities with other entities by using different mechanisms (e.g., contracts and memoranda or letters of agreement). These other entities are public health authorities under the Privacy Rule with respect to the activities they conduct under a grant of authority from such a public health agency. A covered entity may disclose PHI to public health authorities

BOX 4. Examples of situations related to the Privacy Rule and public health

State cancer registry. Under a state law, health-care providers are required to report cancer cases to a state's cancer registry. Names are included to prevent duplicate reporting and counting. State law protects the confidentiality of the data. Can covered entities disclose the information under the Privacy Rule?

Privacy Rule effect. Covered entities may disclose PHI to a public health agency, or any other entity, when the disclosure is required by law. However, as covered entities, the providers must give an accounting to the persons whose PHI has been shared. The state agency may use and further disclose the PHI consistent with applicable state law.

State university-maintained cancer registry. Under a state law, health-care providers are mandated to report cancer cases to a state health department's cancer registry. The state health department contracts with a state university to receive the reports and maintain its registry. As covered entities, can health-care providers disclose PHI to the state university under the Privacy Rule?

Privacy Rule effect. As noted in the previous example, covered entities may disclose, without authorization, PHI to the cancer registry under the Privacy Rule, which expressly permits disclosure of PHI as required by law and sharing of PHI with public health authorities for public health purposes. The state university is acting under a grant of authority from a public health authority, the state health department. The university can use and disclose the information, without authorization, consistent with its agreement with the state health department and applicable state law.

Early hearing detection and intervention. An early hearing detection and intervention program in a state needs data from two large hospitals. The state does not have a law requiring reporting of hearing loss. Under the Privacy Rule, can covered entities release results of newborn hearing-screening tests to the state program?

Privacy Rule effect. The Privacy Rule expressly permits release of PHI, without authorization, from a covered entity to a public health authority (e.g., the state health department), which is authorized by law to receive PHI for the purpose of controlling disease, injury, or disability. The rule does not require a state law mandating such disclosures for PHI to be released to a public health authority. Finally, the covered entities may rely upon the state's representation that the information requested is the minimum necessary for the purposes of the registry.

Disease registry maintained by private foundation. A private foundation maintains a disease registry as a way to support research and service for those with the disease. Can health-care providers release PHI to the foundation under the Privacy Rule?

Privacy Rule effect. Nongovernment disease registries (e.g., those maintained by foundations and other private organizations) are not considered public health authorities unless they have a grant of authority from a public health authority. With such a grant, covered entities may disclose PHI to the foundations. But without a grant of authority, PHI may be released only under one of the following situations:

- Release is authorized by the patient.
- The PHI is de-identified.
- The PHI is contained in a limited data set governed by a data-use agreement.
- Release of PHI is in accord with the rule's provisions for disclosure for research without authorization.
- Release is otherwise permitted by the rule (e.g., to entities subject to the jurisdiction of the Food and Drug Administration (FDA) [45 CFR § 164.512(b)(1)(iii)].

Surveillance project. A state health department that is not a covered entity conducts a surveillance project on human immunodeficiency virus (HIV) and acquired immunodeficiency syndrome (AIDS). The HIV/AIDS surveillance project is an interview study. It asks for self-reported information from participants, including dates of diagnosis and visits for care. Is this PHI covered by the Privacy Rule?

Privacy Rule effect. Information collected directly from persons by a person, agency, or institution that is not a covered entity, including individually identifiable information, is not covered by the Privacy Rule.

and to these designated entities pursuant to the public health provisions of the Privacy Rule.

The Privacy Rule permits covered entities to disclose PHI, without authorization, to public health authorities or other entities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability. This includes the reporting of disease or injury; reporting vital events (e.g., births or deaths); conducting public health surveillance, investigations, or interventions; reporting child abuse and neglect; and monitoring adverse outcomes related to food (including dietary supplements), drugs, biological products, and medical devices [45 CFR 164.512(b)]. Covered entities may report adverse events related to FDA-regulated products or activities to public agencies and private entities that are subject to FDA jurisdiction [45 CFR 164.512(b)(1)(iii)]. To protect the health of the public, public health authorities might need to obtain information related to the individuals affected by a disease. In certain cases, they might need to contact those affected to determine the cause of the disease to allow for actions to prevent further

illness. Also, covered entities may, at the direction of a public health authority, disclose protected health information to a foreign government agency that is acting in collaboration with a public health authority [45 CFR 164.512(b)(1)(i)].

To receive PHI for public health purposes, public health authorities should be prepared to verify their status and identity as public health authorities under the Privacy Rule. To verify its identity, an agency could provide any one of the following:

- if the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
- if the request is in writing, the request is on the appropriate government letterhead;
- if the disclosure is to a person acting on behalf of a public health authority, a written statement on appropriate government letterhead that the person is acting under the government's authority [45 CFR § 164.514(h)(2)].

Public health authorities receiving information from covered entities as required or authorized by law [45 CFR 164.512(a)] [45 CFR 164.512(b)] are not business associates of the covered entities and therefore are not required to enter into business associate agreements. Public health authorities that are not covered entities also are not required to enter into business associate agreements with their public health partners and contractors. Also, after PHI is disclosed to a public health authority pursuant to the Privacy Rule, the public health authority (if it is not a covered entity) may maintain, use, and disclose the data consistent with the laws, regulations, and policies applicable to the public health authority.

Disclosures for Public Health Purposes

The Privacy Rule allows covered entities to disclose PHI to public health authorities when required by federal, tribal, state, or local laws [45 CFR 164.512(a)]. This includes state laws (or state procedures established under such law) that provide for receiving reporting of disease or injury, child abuse, birth, or death, or conducting public health surveillance, investigation, or intervention.

For disclosures not required by law, covered entities may still disclose, without authorization, to a public health authority authorized by law to collect or receive the information for the purpose of preventing or controlling disease, injury, or disability, the minimum necessary information to accomplish the intended public health purpose of the disclosure [45 CFR 164.512 (b)] (Box 1).

For example, to protect the health of the public, public health officials might need to obtain information related to persons affected by a disease. In certain cases, they might need to contact those affected to determine the cause of the disease to allow for actions to prevent further illness. The Privacy Rule continues to allow for the existing practice of sharing PHI with public health authorities who are authorized by law to collect or receive such information to aid them in their mission of protecting the health of the public. Examples of such activities include those directed at the reporting of disease or injury, reporting adverse events, reporting births and deaths, and investigating the occurrence and cause of injury and disease (*1*).

Although it is not a defined term, DHHS interpreted the phrase "authorized by law" to mean that a legal basis exists for the activity. Further, DHHS called the phrase "a term of art," including both actions that are permitted and actions that are required by law [64 FR 59929, November 3, 1999]. This does not mean a public health authority at the federal, tribal, state, or local level must have multiple disease or condition-specific laws that authorize each collection of information. Public health authorities operate under broad mandates to protect the health of their constituent populations.

Requirements for Covered Entities

Accounting for Public Health Disclosures

Although the Privacy Rule permits disclosures of PHI to public health authorities, covered entities must comply with certain requirements related to these disclosures. One such requirement is that a covered entity must be able to provide an individual, upon request, with an accounting of certain disclosures of PHI. The covered entity is not required to account for all disclosures of PHI. For example, an accounting is not required for disclosures made

- prior to the covered entity's compliance date;
- for TPO purposes;
- to the individual or pursuant to the individual's written authorization; or
- as part of a limited data set.

However, usually an accounting is required for disclosures made without authorization, including public health purposes.

The required accounting for disclosures may be accomplished in different ways. Typically, the covered entity must provide the individual with an accounting of each disclosure by date, the PHI disclosed, the identity of the recipient of the PHI, and the purpose of the disclosure. However, where the covered entity has, during the accounting period, made multiple disclosures to the same recipient for the same purpose, the Privacy Rule provides for a simplified means of accounting. In such cases, the covered entity need only identify the recipient of such repetitive disclosures, the

purpose of the disclosure, and describe the PHI routinely disclosed. The date of each disclosure need not be tracked. Rather, the accounting may include the date of the first and last such disclosure during the accounting period, and a description of the frequency or periodicity of such disclosures. For example, the vast amount of data exchanged between covered entities and public health authorities is made through ongoing, regular reporting or inspection requirements. A covered health-care provider may routinely report all cases of measles it diagnoses to the local public health authority. An accounting of such disclosures to a requesting individual would need to identify the local public health authority receiving the PHI, the PHI disclosed, the purpose of the disclosure (required for communicable disease surveillance), the periodicity (weekly), and the first and last dates of such disclosures during the accounting period (May 1, 2003 to June 1, 2003). Thus, the covered entity would not need to annotate each patient's medical record whenever a routine public health disclosure was made.

Notice of Privacy Practices

With certain exceptions, under the Privacy Rule, individuals have the right to adequate notice of the uses and disclosures of PHI that may be made by the covered entity, as well as their rights and the covered entity's legal obligations. Notices must be in plain language and clearly posted. Certain covered entities must make a good faith effort to obtain an individual's acknowledgment of receipt of this notice. In certain cases, notice may be provided electronically.

Minimum Necessary Standard

The Privacy Rule usually directs covered entities to limit the amount of information disclosed to the minimum necessary to achieve the specified goal [45 CFR § 164.514(d)(1)]. This requirement usually applies to disclosures to a public health agency. It would not apply, however, if the disclosure were required by law, authorized by the individual, or for treatment purposes. A covered entity may also reasonably rely on a public official's determination that the information requested is the minimum necessary for the public health purpose.

Public Health Authorities Performing Covered Functions

Public health authorities at the federal, tribal, state, or local levels that perform covered functions (e.g., providing health care or insuring individuals for health-care costs), may be subject to the Privacy Rule's provisions as covered entities. For example, a local public health authority that operates a health clinic providing essential health-care services to low-income persons and performs certain electronic transactions might be defined under the Privacy Rule as a covered health-care provider and therefore a covered entity. Flow charts and interactive tools designed to help determine covered entity status are provided online by the Centers for Medicare and Medicaid Services, available at http://www.cms.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp.

The following are examples of public health authority functions that make them covered entities:

- **Public health authorities as covered health-care providers.** A public health authority that conducts health care as part of its activities is a covered health-care provider if it also performs electronic transactions covered by the HIPAA Transactions Rule as part of these activities. The fact that these activities are conducted in pursuit of a public health goal (e.g., vaccinating children or screening a targeted population for sexually transmitted diseases) does not preclude the public health authority from being a covered entity.
- **Public health authorities as health plans.** Under the Privacy Rule, a health plan is an individual or group plan that provides, or pays the cost of, medical care. This specifically includes government health plans (e.g., Medicare, Medicaid, or Veterans Health Administration). However, the Privacy Rule defines health plan to exclude government-funded programs whose principal activity is the direct provision of health care to persons or the making of grants to fund the direct provision of health care to persons [45 CFR § 160.103]. Examples include the Ryan White Comprehensive AIDS Resources Emergency Act. Although certain government programs that fund providers directly may not be health plans, government programs that reimburse providers or otherwise fund providers to perform direct health-care services should carefully analyze the details of their programs to determine if they are performing covered functions.
- **Public health authorities as health-care clearinghouses.** Although unlikely, a public health authority might be a health-care clearinghouse if it receives health information from another entity and translates that information from a nonstandard format into a standard transaction or standard data elements (or vice versa). Operators of community health information systems should carefully consider whether they meet the definition for a health-care clearinghouse.
- **Public health agencies as hybrid entities.** A public health agency that is a covered entity, and has both covered and noncovered functions may become a hybrid entity by designating its health-care components. By designating itself as a hybrid entity, a public health authority can carve out its noncovered functions, so that the majority of Privacy

Rule provisions apply only to its health-care component, which is required to comply with the Privacy Rule requirements, including using and disclosing PHI only as authorized, meeting the administrative requirements, accounting for disclosure of PHI, and providing a notice of practices. However, such a designation does not preclude the public health authority from continuing to conduct authorized public health functions. A covered entity that is also a public health authority may use, as well as disclose, PHI for public health purposes to the same extent it would be permitted to disclose the PHI as a public health authority.

The Privacy Rule and Public Health Research

The topic of research under the Privacy Rule is covered in depth in the DHHS report, Protecting Personal Health Information in Research — Understanding the HIPAA Privacy Rule (*6*). The Privacy Rule provides separate provisions for disclosure without individual authorization for public health purposes and for certain research [45 CFR § 164.512(b)] [45 CFR § 164.512(i)]. Other federal law pertaining to research stresses the importance of distinguishing between research and practice to ensure that human subjects are appropriately protected [45 CFR Part 46]. For certain activities, this distinction is not always clear. A full discussion of the distinctions between public health practice and research is beyond the scope of this document. However, CDC and others provide guidance in this area (*7–9*).

Research Versus Practice

The definition of research is the same for the Privacy Rule and the Common Rule (*10*) — systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. Research is designed to test a hypothesis, permit conclusions to be drawn, and thereby to develop or contribute to generalizable knowledge. The majority of public health activities (e.g., public health surveillance, and disease prevention and control projects) are based on scientific evidence and data collection or analytic methods similar to those used in research. However, they are not designed to contribute to generalizable knowledge. Their primary purpose is to protect the health of the population through such activities as disease surveillance, prevention, or control.

The Belmont Report (*11*) defines practice as interventions designed solely to enhance the well-being of a person, patient, or client, and which have reasonable expectation of success. The report further states that the purpose of medical or behavioral practice is to provide diagnosis, preventive treatment, or therapy to particular patients. For public health agencies, the patient is the community. Public health practice activities (e.g., public health surveillance, disease control, or program evaluation) are undertaken with the intent to benefit a specific community, although occasionally they may provide unintended generalizable benefits to others.

Some public health activities that are initially public health practice may subsequently evolve into a research activity (e.g., an investigation to determine the cause of an outbreak that incorporates a research study evaluating the efficacy of a new drug to treat the illness). When that is the case, the disclosures may be made initially under the public health provisions of the Privacy Rule. But when the activity becomes an ongoing research activity, the entity should consider application of the relevant research disclosures provisions to continue to obtain information for this purpose. Moreover, there may be cases where the activity is both research and public health practice (e.g., an ongoing survey to monitor health conditions in the population, data from which can also be analyzed for research purposes). In those cases, disclosures may be made either under the research provisions or the public health provisions, as appropriate — the covered entity need not comply with both sets of requirements.

The Privacy Rule and Other Laws

- **Federal laws.** Covered entities subject to the Privacy Rule are also subject to other federal statutes and regulations. The specific relationship of the Privacy Rule and certain federal laws is discussed in the preamble to the December 2000 Final Rule [65 Fed.Reg. 82481]. In certain instances, the Privacy Rule imposes requirements in direct conflict with other federal laws or regulations. In those instances, an analysis will be necessary to determine whether the later provision was intended to overrule the prior law or regulation.
- **State laws.** As a federal regulatory standard, the Privacy Rule preempts only those contrary state laws relating to the privacy of individually identifiable health information that have less stringent requirements or standards than the Privacy Rule (i.e., more stringent laws remain in effect). In addition, DHHS may, upon specific request from a state or other entity or person, determine that a provision of state law that is contrary to the federal requirements and that meets certain additional criteria, will not be preempted by the federal requirements. Thus,

preemption of a contrary state law will not occur if the Secretary or designated DHHS official determines, in response to a request, that the state law 1) is necessary to prevent fraud and abuse related to the provision of or payment for health care; 2) is necessary to ensure appropriate state regulation of insurance and health plans to the extent expressly authorized by statute or regulation; 3) is necessary for state reporting on health-care delivery or costs; 4) is necessary to serve a compelling public health, safety, or welfare need, and, if a Privacy Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or 5) has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances. The Privacy Rule specifically does not preempt contrary state public health laws that provide for the reporting of disease or injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation, or intervention [45 CFR § 160.202].

Online Resources

References to non-DHHS sites on the Internet are provided as a service to *MMWR* readers and do not constitute or imply endorsement of these organizations or their programs by CDC or the U.S. Department of Health and Human Services. CDC is not responsible for the content of these sites. URL addresses listed in *MMWR* were current as of the date of publication.

Federal Government Resources

DHHS Office for Civil Rights — HIPAA guidelines
http://www.hhs.gov/ocr/hipaa
CDC — Privacy Rule guidelines
http://www.cdc.gov/privacyrule
Centers for Medicare and Medicaid Services
http://www.cms.gov/hipaa/
http://www.cms.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp
Health Resources and Services Administration — HIPAA
http://www.hrsa.gov/website.htm
National Center for Health Statistics
http://www.cdc.gov/nchs/otheract/phdsc/phdsc.htm
National Committee on Vital and Health Statistics
http://www.ncvhs.hhs.gov/
National Health Information Infrastructure
http://www.health.gov/ncvhs-nhii/
Indian Health Service — HIPAA
http://www.ihs.gov/AdminMngrResources/HIPAA/index.cfm
National Institutes of Health
http://privacyruleandresearch.nih.gov
Substance Abuse and Mental Health Services Administration — HIPAA
http://www.samhsa.gov/hipaa/

State Government Resources

California
http://www.dhs.ca.gov/hipaa/
http://www.ohi.ca.gov/state/calohi/ohiHome.jsp
http://www.dmh.ca.gov/hipaa/
Colorado
http://www.cdphe.state.co.us/HIPAA/
Florida
http://www.myflorida.com/myflorida/sto/hipaa/
Illinois
http://www.state.il.us/dpa/hipaa.html
Kentucky
http://chs.state.ky.us/dms/HIPAA/default.htm
http://dmhmrs.chr.state.ky.us/hipaa.asp
Maryland
http://www.mhcc.state.md.us/edi/hipaa/_hipaa.htm
http://dhmh.state.md.us/HIPAA/
Minnesota
http://www.dhs.state.mn.us/hipaa/
Missouri
http://www.health.state.mo.us/HIPAA/
New York
http://www.oft.state.ny.us/hipaa/index.htm
North Carolina
http://dirm.state.nc.us/hipaa/
Ohio
http://www.state.oh.us/hipaa/
Pennsylvania
http://www.dpw.state.pa.us/omap/hipaa/omaphipaa.asp
http://www.insurance.state.pa.us/html/hipaa.html
South Carolina
http://www.hipaa.state.sc.us/
Texas
http://www.hhsc.state.tx.us/NDIS/NDISTaskForce.html
Virginia
http://www.dmas.state.va.us/hpa-home.htm
Wisconsin
http://www.dhfs.state.wi.us/HIPAA/

Associations, Nonprofit Organizations, and Academic Resources

American Hospital Association — HIPAA
http://www.hospitalconnect.com/aha/key_issues/hipaa/resources/resources.html

American Medical Association — HIPAA
http://www.ama-assn.org/ama/pub/category/4234.html

Association of State and Territorial Health Officials — HIPAA
http://www.astho.org/?template=hipaa.html

Georgetown University Health Privacy Project
http://www.healthprivacy.org/

Joint Healthcare Information Technology Alliance
http://www.jhita.org/

National Association of Health Data Organizations
http://www.nahdo.org/

National Association of Insurance Commissioners
http://www.naic.org/1privacy/initiatives/health_privacy.htm

National Governors Association — HIPAA
http://www.nga.org/center/topics/1,1188,C_CENTER_ISSUE^D_4324,00.html

North Carolina Healthcare Information and Communications Alliance
http://www.nchica.org/

Public Health Grand Rounds HIPAA Privacy Rule: Enhancing or Harming Public Health?
http://www.publichealthgrandrounds.unc.edu/

Stanford University Medical School — HIPAA
http://www.med.stanford.edu/HIPAA/

Workgroup for Electronic Data Interchange — Strategic National Implementation Process
http://www.wedi.org/snip/

Acknowledgments

This report was prepared by Salvatore Lucido, M.P.A., and Denise Koo, M.D., Office of the Associate Director for Science, Epidemiology Program Office, CDC, in collaboration with James G. Hodge, Jr., J.D., Center for Law and the Public's Health, Georgetown and Johns Hopkins Universities, Baltimore, Maryland. The preparers are grateful for the participation of Deborah Tress, J.D., Kenya Ford, J.D., and Heather Horton, J.D., Office of the General Counsel, Department of Health and Human Services, CDC/ATSDR Branch; the CDC Working Group on the Privacy Rule; and Beverly Dozier, J.D., Lance A. Gable, J.D., Lawrence O. Gostin, J.D., Gail Horlick, J.D., and Jennifer Kurle.

The preparers also thank the following partners for their valuable input: Association of State and Territorial Health Officers, Council of State and Territorial Epidemiologists, National Association of County and City Health Officials, National Association of Health Data Organizations, Association of Public Health Laboratories, and National Association for Public Health Statistics and Information Systems.

References

1. Gostin LO, Hodge JG Jr. Personal privacy and common goods: a framework. Minnesota Law Review 2002;86:1439–80.
2. Health Insurance Portability and Accountability Act of 1996. Pub. L. No. 104-191, 110 Stat. 1936 (1996).
3. Office for Civil Rights, Department of Health and Human Services. Title 45 of the Code of Federal Regulations Parts 160 and 164. Available at http://www.dhhs.gov/ocr/combinedregtext.pdf.
4. Office for Civil Rights. OCR guidance explaining significant aspects of the Privacy Rule, 2002. Department of Health and Human Services. Available at http://www.hhs.gov/ocr/hipaa.
5. Gostin, LO, Hodge JG Jr. Privacy Law Advisory Committee. Model state public health information privacy act, 1999. Available at http://www.publichealthlaw.net/Resources/ResourcesPDFs/modelprivact.pdf.
6. Department of Health and Human Services. Protecting personal health information in research — understanding the HIPAA Privacy Rule. Department of Health and Human Services. Washington, D.C.: 2003 (in press).
7. Snider DE, Stroup DF. Defining research when it comes to public health. Public Health Rep 1997:112:29–32.
8. CDC. Guidelines for defining public health research and public health nonresearch. Available at http://www.cdc.gov/od/ads/opspoll1.htm.
9. Amoroso PJ, Middaugh JP. Research vs. public health practice: when does a study require IRB review? Prev Med 2003;36:250–3.
10. Office for Protection from Research Risks, National Institutes of Health, Department of Health and Human Services. Public welfare: protection of human subjects, 2001. [45 CFR 46]. Available at http://ohrp.osophs.dhhs.gov/humansubjects/guidance/45cfr46.htm.
11. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. Belmont report: ethical principles and guidelines for the protection of human subjects of research. Department of Health, Education and Welfare. Available at http://www.med.umich.edu/irbmed/ethics/belmont/BELMONTR.HTM.

Appendix A

Selected Privacy Rule Concepts and Definitions

The following concepts and definitions are adapted from the regulatory language. For further information, see the citations to the Privacy Rule.

Accounting. An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures (a) to carry out treatment, payment and health care operations [45 CFR § 164.506]; (b) to individuals of protected health information about them [45 CFR § 164.502]; (c) incident to a use or disclosure otherwise permitted or required by this subpart, as provided in 45 CFR §164.502; (d) pursuant to an authorization as provided in 45 CFR §164.508; (e) for the facility's directory or to persons involved in the individual's care or other notification purposes, as provided in 45 CFR §164.510; (f) for national security or intelligence purposes as provided in 45 CFR §164.512(k)(2), (g) to correctional institutions or law enforcement officials as provided in 45 CFR §164.512 (k)(5); or (h) as part of a limited data set in accordance with 45 CFR §164.514(e); or (i) that occurred prior to the compliance date for the covered entity…. Such an accounting must meet the following requirements: (1) except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity; (2) except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must include for each disclosure: the date of the disclosure, the name of the entity or person who received the protected health information, and if known, the address of such entity or person; a brief description of the protected health information disclosed; and, a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or in lieu of such a statement, a copy of the individual's written authorization pursuant to 45 CFR § 164.508, or a copy of a written request for a disclosure under 45 CFR § 164.502(a)(2)(ii) or 45 CFR § 164.512, if any.

If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under 45 CFR § 164.502(a)(2)(ii) or 45 CFR § 164.512, the accounting may, with respect to such multiple disclosures, provide the information required by paragraph (b)(2) of 45 CFR § 164.528 for the first disclosure during the accounting period, the frequency, periodicity, or number of the disclosures made during the accounting period, and the date of the last such disclosure during the accounting period [45 CFR § 164.528].

Modified accounting procedures are also provided for covered entities making research disclosures involving >50 persons [45 CFR § 164.528(b)(4)].

Business associate. A person who, on behalf of a covered entity or of an organized health care arrangement [45 CFR § 154.501] in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of . . . a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or any other function or activity regulated by this subchapter; or provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation [45 CFR § 164.501], management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health-care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the individual [45 CFR § 160.103].

Covered entity. 1) a health plan; 2) a health-care clearinghouse; 3) a health-care provider who transmits any health information in electronic form in connection with a transaction [45 CFR § 160.103].

Covered functions. Those functions of a covered entity the performance of which makes the entity a health plan, health-care provider, or health-care clearinghouse [45 CFR § 164.103].

Data aggregation. With respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another

covered entity, to permit data analyses that relate to the health-care operations of the respective covered entities [45 CFR §164.501].

De-identified health information. Health information that does not identify an individual and with respect to which no reasonable basis exists to believe that the information can be used to identify an individual is not individually identifiable information. [45 CFR § 164.514(a)].

Disclosure. The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information [45 CFR § 160.103].

Electronic media. 1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or 2) transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission [45 CFR § 160.103].

Health care. Care, services, or supplies related to the health of an individual. It includes but is not limited to 1) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and, 2) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription [45 CFR § 160.103].

Health-care clearinghouse. A public or private entity, including a billing service, repricing company, community health management information system, community health information system, or value-added network or switch that 1) processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction or 2) receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity [45 CFR § 160.103].

Health-care operations. Any of the following activities of the covered entity to the extent that the activities are related to covered functions: 1) conducting quality assessment and improvement activities, population-based activities, and related functions that do not include treatment; 2) reviewing the competence or qualifications of health care professionals, evaluating practitioner, provider, and health plan performance, conducting training programs where students learn to practice or improve their skills as health-care providers, training of nonhealth-care professionals, accreditation, certification, licensing, or credentialing activities; 3) underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or benefits; 4) conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; 5) business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and 6) business management and general administrative activities of the entity [45 CFR § 164.501].

Health-care provider. A provider of services, (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health-care services, (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other individual or organization that furnishes, bills, or is paid for health care in the normal course of business [45 CFR § 160.103].

Health information. Any information, whether oral or recorded in any form or medium, that 1) 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 2) 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 [45 CFR § 160.103].

Health plan. An individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)). Health plan includes the following, singly or in combination: (i) a group health plan as defined in 45 CFR § 160.103 of the Privacy Rule; (ii) a health insurance issuer, as defined in 45 CFR § 160.103 of the Privacy Rule; (iii) an HMO, as defined in 45 CFR § 160.103 of the Privacy Rule; (iv) Part A or B of the Medicare program under title XVIII of the Act; (v) the Medicaid program under title XIX of the Act, 42 U.S.C. 1396 et seq.; (vi) an issuer of a Medicare supplemental policy, (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)); (vii) an issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy; (viii) an employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more

employers; (ix) the health care program for active military personnel under title 10, U.S.C.; (x) the veterans health-care program under 38 U.S.C. Ch. 17; (xi) the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)); (xii) the Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.; (xiii) the Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.; (xiv) an approved state child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act; 42 U.S.C. 1397, et seq.; (xv) the Medicare+Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28; (xvi) a high risk pool that is a mechanism established under state law to provide health insurance coverage or comparable coverage to eligible individuals; (xvii) any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)) [45 CFR § 160.103].

The term health plan excludes: (i) any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in §2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and, (ii) a government-funded program, other than the one listed in items (i)-(xvi) above, whose principal purpose is other than providing, or paying the cost of, health care, or whose principal activity is 1) the direct provision of health care to individuals; or 2) the making of grants to fund the direct provision of health care to individuals [45 CFR § 160.103].

Hybrid entity. A single legal entity 1) that is a covered e ntity; 2) whose business activities include both covered and noncovered functions; and 3) that designates its health-care components [45 CFR § 164.103].

Individually identifiable health information. A subset of health information, including demographic information collected from an individual, and 1) is created or received by a health-care provider, health plan, employer, or health-care clearinghouse; and, 2) 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; and, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual [45 CFR § 164.501].

Limited data set. Protected health information that excludes certain direct identifiers of the individual or of relatives, employers, or household members of the individual. Direct identifiers to be excluded can be found in 45 CFR § 164.514(e)(2).

Minimum necessary. For any type of disclosure that a covered entity makes on a routine and recurring basis, that the covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. For all other disclosures, covered entities must develop and implement criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought and review requests for disclosure on an individual basis in accordance with such criteria. A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when (a) making disclosures to public officials that are permitted under 45 CFR § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose, (b) if the information is requested by another covered entity (c) their business associates providing personal services, or (d) documentation or representations that comply with the applicable requirements of 45 CFR § 164.512(i) have been provided by an individual requesting the information for research purposes [45 CFR § 164.514(d)(3)].

The minimum necessary standard also applies to uses of protected health information [45 CFR § 164.514(d)(2)] and requests for protected health information [45 CFR § 164.514(d)(4)].

Notice. An individual, with certain exceptions, has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity and of the individual's rights, and the covered entity's legal duties, with respect to protected health information. The notice must be written in plain language and contain the following elements: (i) a header as specified in the rule; (ii) a description, including at least one example, of the types of uses and disclosures that the covered entity is permitted to make for treatment, payment, and health care operations, and a description of each of the other purposes for which the covered entity is permitted or required to use or disclose protected health information without the individual's written consent or authorization. If a use or disclosure is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law (as defined in 45 CFR § 160.202). Each description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by the Privacy Rule or other applicable law, and a statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as provided by 45 CFR § 164.508(b)(5).

A separate statement must be included in the notice if a covered entity intends to engage in any of the following activities. The statement should explain that 1) the covered entity may contact the individual to provide appointment reminders or information regarding treatment alternatives or other health-related benefits; 2) the covered entity may contact the individual to raise funds for the covered entity; or 3) a group health plan, health insurer, or HMO with respect to a group health plan may disclose protected health information to the sponsor of the plan.

The notice must contain a statement of the individual's rights with respect to the protected health information and a brief description of how the individual may exercise these rights, a statement of the covered entity's duties, a statement that individuals may complain to the covered entity or the Secretary if they believe their privacy rights have been violated, contact information, and the effective date of the notice [45 CFR § 164.520].

Payment. 1) The activities undertaken by (i) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (ii) a health-care provider or health plan to obtain or provide reimbursement for the provision of health care; and 2) the activities relate to the individual to whom health care is provided and include, but are not limited to (i) determinations of eligibility or coverage and adjudication or subrogation of health benefit claims; (ii) risk adjusting amounts due based on enrollee health status and demographic characteristics; (iii) billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance) and related health-care data processing; (iv) review of health-care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (v) utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (vi) disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement: (a) name and address; (b) date of birth; (c) social security number; (d) payment history; (e) account number; and (f) name and address of the health-care provider or health plan [45 CFR § 164.501].

Protected health information (PHI). Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes individually identifiable health information in: (i) education records covered by the Family Education Rights and Privacy Act (20 U.S.C. 1232g); (ii) records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) employment records held by a covered entity in its role as employer [45 CFR § 160.103].

Public health authority. An agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or an individual or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or individuals or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate [45 CFR § 164.501].

Examples of public health authorities include state and local health departments, CDC, National Institutes of Health (NIH), Food and Drug Administration (FDA), and Occupational Safety and Health Administration (OSHA).

Required by law. A mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. This term includes, but is not limited to court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health-care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits [45 CFR § 164.103].

Research. A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge [45 CFR § §164.501].

Statistical de-identification. A properly qualified statistician using accepted analytical techniques concludes that the risk is limited that the information could be used, alone or in combination with other reasonably available information to identify the subject of the information [45 CFR § 164.514(b)].

Safe harbor method. A covered entity or its agent removes a comprehensive set of identifiers enumerated in the Privacy Rule, which includes but is not limited to, names, geographic subdivisions smaller than states, dates more specific than years, contact information, identification numbers and photographic images, and has no actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual who is a subject of the information, or the individual's relatives, employers, or household members. Eighteen specific identifiers will need to be removed to achieve de-identification [45 CFR § 164.514(b)].

Transaction. The transmission of information between two parties to carry out financial or administrative activities

related to health care. It includes the following types of information transmissions: health care claims or equivalent encounter information; health care payment and remittance advice; coordination of benefits; health care claim status; enrollment and disenrollment in a health plan; eligibility for a health plan; health plan premium payments; referral certification and authorization; first report of injury; health claims attachments; and other transactions that the Secretary may prescribe by regulation [45 CFR § 164.103].

Treatment. The provision, coordination, or management of health care and related services by one or more health-care providers, including the coordination or management of health care by a health-care provider with a third party; consultation between health-care providers relating to a patient; or the referral of a patient for health care from one health-care provider to another [45 CFR § 164.501].

Use. With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information [45 CFR § 160.103].

Appendix B

Sample Text That Can Be Used To Clarify Public Health Issues Under the Privacy Rule

Following are sample letters that can be used to help clarify Privacy Rule issues among covered entities and public health authorities (e.g., CDC, National Institutes of Health, Food and Drug Administration, Substance Abuse and Mental Health Services Administration, Health Resources and Services Administration, state and local health departments). Public health authorities can use these letters as templates by inserting names of the appropriate individuals, projects, agreements, laws, activity types, covered entities, public health authorities, and authorized agencies.

From a public health authority to a covered entity, clarifying rules regarding disclosure

To Whom it May Concern:

[Public health authority] is an agency of [parent authority] and is conducting the activity described here in its capacity as a public health authority as defined by the Health Insurance Portability and Accountability Act (HIPAA), Standards for Privacy of Individually Identifiable Health Information; Final Rule (Privacy Rule) [45 CFR §164.501]. Pursuant to 45 CFR §164.512(b) of the Privacy Rule, covered entities such as your organization may disclose, without individual authorization, protected health information to public health authorities " . . . authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions . . . "

[Public health authority] is conducting [project], a public health activity as described by 45 CFR § 164.512(b), and is authorized by [law or regulation]. The information being requested represents the minimum necessary to carry out the public health purposes of this project pursuant to 45 CFR §164.514(d) of the Privacy Rule.

If you have questions or concerns please contact [project leader].

From a public health authority to an authorized agency, providing grant of authority

Dear [authorized agency]:

This letter serves as verification of a grant of authority from [public health authority] for you to conduct the public health activities described here, acting as a public health authority pursuant to the Standards for Privacy of Individually Identifiable Health Information promulgated under the Health Insurance Portability and Accountability Act (HIPAA) [45 CFR Parts 160 and 164)]. Under this rule, covered entities may disclose, without individual authorization, protected health information to public health authorities " . . . authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions . . . ." The definition of a public health authority includes " . . . an individual or entity acting under a grant of authority from or contract with such public agency . . . ."

[Authorized agency] is acting under [contract, grant, cooperative agreement] with [public health authority] to conduct [project], which is authorized by [law or regulation]. [Public health authority] grants this authority to [authorized agency] for purposes of this project. Further, [public health authority] considers this to be [activity type], for which disclosure of protected health information by covered entities is authorized by 45 CFR § 164.512(b) of the Privacy Rule.

From a public health authority to a covered entity, confirming grant of authority to an authorized agency

To Whom It May Concern:

[Public health authority] is an agency of [parent authority] and is a public health authority as defined by the Health Insurance Portability and Accountability Act (HIPAA), Standards for Privacy of Individually Identifiable Health Information; Final Rule (Privacy Rule)[45 CFR § 164.501]. Pursuant to 45 CFR § 164.512(b) of the Privacy Rule, covered entities may disclose protected health information to public health authorities " . . . authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions . . . ." The definition of public health authority includes " . . . an individual or entity acting under a grant of authority from or contract with such public agency . . ." [45 CFR § 164.501]. [Authorized agency] is acting under [contract, grant or cooperative agreement] with [public health authority] to carry out [project].

Through this grant of authority, [authorized agency] may function as a public health authority under the Privacy Rule for purposes of this project.

[Project] is a public health activity as described by 45 CFR § 164.512(b) referenced previously, and is authorized by [law or regulation]. The information being requested represents the minimum necessary to carry out the public health purposes of this project pursuant to 45 CFR § 164.514(d) of the Privacy Rule. The Privacy Rule provides that covered entities " . . . may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purposes when making disclosures to public officials that are permitted under 45 CFR § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purposes(s)."

If you have questions or concerns please contact [project leader for authorized agency; public health authority contact].

All *MMWR* references are available on the Internet at http://www.cdc.gov/mmwr. Use the search function to find specific articles.

Use of trade names and commercial sources is for identification only and does not imply endorsement by the U.S. Department of Health and Human Services.

References to non-CDC sites on the Internet are provided as a service to *MMWR* readers and do not constitute or imply endorsement of these organizations or their programs by CDC or the U.S. Department of Health and Human Services. CDC is not responsible for the content of these sites. URL addresses listed in *MMWR* were current as of the date of publication.

The *Morbidity and Mortality Weekly Report (MMWR)* series is prepared by the Centers for Disease Control and Prevention (CDC) and is available free of charge in electronic format and on a paid subscription basis for paper copy. To receive an electronic copy each week, send an e-mail message to *listserv@listserv.cdc.gov*. The body content should read *SUBscribe mmwr-toc*. Electronic copy also is available from CDC's Internet server at *http://www.cdc.gov/mmwr* or from CDC's file transfer protocol server at *ftp://ftp.cdc.gov/pub/publications/mmwr*. To subscribe for paper copy, contact Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402; telephone 202-512-1800.

Data in the weekly *MMWR* are provisional, based on weekly reports to CDC by state health departments. The reporting week concludes at close of business on Friday; compiled data on a national basis are officially released to the public on the following Friday. Address inquiries about the *MMWR* series, including material to be considered for publication, to Editor, *MMWR* Series, Mailstop C-08, CDC, 1600 Clifton Rd., N.E., Atlanta, GA 30333; telephone 888-232-3228.

All material in the *MMWR* series is in the public domain and may be used and reprinted without permission; however, citation of the source is appreciated.

☆U.S. Government Printing Office: 2003-533-155/69108 Region IV