Drug Abuse Warning Network

The D·A·W·N report

AUGUST 2001

Health Information Privacy and DAWN

Can a hospital comply with HIPAA and continue to participate in DAWN?

This is the question that hospital participants in the Drug Abuse Warning Network (DAWN) have been asking. This edition of *The DAWN Report* explains why the answer is **Yes**.

New health information privacy regulations affecting most, possibly all, hospital participants in DAWN were published on December 28, 2000 (*65 Federal Register* 82462). These rules became effective April 14, 2001. Health care providers, health plans, and health care clearinghouses have 2 years—until April 14, 2003 (2004 for small health plans)—to comply.

Some questions have arisen about how these regulations apply in day-to-day operations. Over the past year, DAWN staff have received many questions from hospital participants and DAWN reporters about the impact of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) on DAWN participation.

The purpose of this report is to provide an overview of HIPAA—in particular, the HIPAA privacy regulations—and describe their applicability to DAWN. To do this, we:

- Summarize the relevant provisions of HIPAA as they relate to DAWN hospitals,
- Present the information in an easy-to-use question-and-answer format, and
- Identify reliable sources for additional information.

This is not intended to be a comprehensive review of the HIPAA requirements. For example, many exceptions to the privacy standards (e.g., for emergency situations) are not covered in this review. However, this brief report is designed to answer many of the key questions being posed by DAWN participants.

Inside

The DAWN Report is published periodically by the Office of Applied Studies, Substance Abuse and Mental Health Services Administration (OAS/SAMHSA).
The author of this report is Judy K. Ball, Ph.D., M.P.A. who is the OAS/SAMHSA Team Leader for the Drug Abuse Warning Network (DAWN). Dr. Ball has participated in the Department of Health and Human Services (DHHS) implementation of administrative simplification under HIPAA since 1997.

What is Administrative Simplification?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is best known for its provisions to increase the portability of health insurance from job to job. Less well known, but with far greater potential benefit for the entire health care system, are the "Administrative Simplification" provisions of HIPAA. The goal of administrative simplification is improving the efficiency and effectiveness of the health care system. The means to achieve this goal is the adoption of national standards to enable efficient, electronic health care transactions.

Administrative simplification has three components:
- Electronic transactions,
- Identifiers for use in the health care system, and
- Security and privacy.

These 3 components are intended to work together like the legs of a 3-legged stool. Each is essential for administrative simplification to work; alteration of any leg affects the integrity of the whole. Electronic transactions need identifiers for accurate and parsimonious addressing. Security and privacy protections are essential to protect sensitive health information whether it is in motion—part of a transaction going from sender to receiver—or at rest—residing in an electronic database or in a file cabinet. Protection involves limiting access to those with a need to know and ensuring the integrity of the information as well.

What electronic transaction standards have been adopted under HIPAA?

Final regulations published August 17, 2000, adopted standards for 8 transactions:
- Health claims and equivalent encounter information,
- Enrollment and disenrollment in a health plan,
- Eligibility for a health plan,
- Health care payment and remittance advice,
- Health plan premium payments,
- Health claim status,
- Referral certification and authorization, and
- Coordination of benefits.

For health care transactions other than retail pharmacy, the standards adopted are those developed by the accredited standards committee (ASC) X12N. For retail pharmacy, the standards adopted are those developed by the National Council for Prescription Drug Programs (NCPDP).

Compliance with these transaction standards is required by October 16, 2002 (2003 for small health plans).

Other transactions—for example, for claims attachments—will be adopted at a later date. HIPAA gives the U.S. Department of Health and Human Services (HHS) authority to adopt additional transactions that will contribute to the efficiency and effectiveness of the health care system.

What identifiers are required by HIPAA?

HIPAA requires the adoption of 4 identifiers, for:
- Health care providers,
- Health plans,
- Employers, and
- Individuals.

A proposed rule to adopt the National Provider Identifier was published on May 7, 1998. A proposed rule to adopt the Employer Identification Number (EIN) as the employer identifier under HIPAA was published June 16, 1998.

Final rules for the National Provider Identifier and the employer identifier are under development. A proposal for the health plan identifier is also under development.

All work on the individual identifier was suspended in 1998 because of the lack of Federal privacy protections at that time.

ormation Privacy under HIPAA

Why did HHS create privacy regulations?

Privacy regulations were required by law.

First, HIPAA required HHS to make recommendations to the Congress for comprehensive Federal privacy legislation. Those recommendations were submitted to Congress on September 11, 1997.

Second, if Congress did not enact privacy legislation by August 21, 1999, HIPAA required HHS to publish privacy regulations. Many privacy bills were considered in Congress, but none passed by the deadline, so HHS had to publish privacy regulations.

What information is covered?

Individually identifiable health information in any form or medium—paper or electronic—is covered under the privacy regulations. Collectively, such information is called "protected health information."

Once information is de-identified—that is, once individual identifying information has been removed—it is no longer protected under these rules.

Who must comply?

Three groups of "covered entities" must comply:
- All health plans,
- Health care clearinghouses, and
- Health care providers that transmit any information in connection with a covered transaction.

Hospitals that choose to conduct transactions (e.g., submit claims electronically to a health plan) will be required to use the HIPAA standard transactions, and by virtue of using the transactions, these hospitals become covered entities under the privacy rule. Currently, most hospitals submit electronic claims to Medicare. If hospitals continue to submit electronic claims, they will be covered entities and subject to the privacy rules.

What is a use? What is a disclosure?

Use refers to information used within the entity that maintains the information.

A disclosure occurs when the information travels outside the entity that holds the information.

Most covered entities will have multiple components. In general, a barrier must be erected to prevent disclosures between the health care and nonhealth care components. Health care components (e.g., the emergency department [ED], the medical records department) hold and maintain protected health information and need to have access to such information, while other, nonhealth care components (e.g., a personnel department, a hospital's facility maintenance department) must be prevented from having access.

A covered entity may use or disclose protected information to a business associate that performs functions on its behalf and the restrictions on uses and disclosures follow the information. The covered entity must establish a contract with its business associate(s) to prevent improper uses or disclosures by the business associate.

How much information can be used or disclosed?

For uses and disclosures of protected health information, the "minimum necessary" standard applies in most instances. That is, a covered entity must make a reasonable effort to use or disclose only the minimum amount of information necessary to fulfill the purpose. As a general rule, disclosing an entire medical record in anticipation of requests for more information would exceed the minimum necessary standard.

Similarly, a covered entity requesting information is required to limit its request to the minimum amount of information necessary to fulfill the purpose. In this way, one covered entity is not responsible for policing the minimum necessary determinations of other covered entities.

For uses, covered entities must define role-based access rules differentiating types of workers, types of information, and the conditions of use.

For disclosures, covered entities must develop rules and protocols for disclosures that are routine and recurring. They need to develop criteria to apply to nonroutine disclosures on a case-by-case basis.

Uses and disclosures for treatment are important exceptions to the minimum necessary rule. The intent is to facilitate a free flow of information necessary for treatment, where restricting information could jeopardize quality of care.

De-identified information (discussed below) is not subject to these rules.

What disclosures are required?

Only 2 types of disclosures of protected health information are required:
- Disclosures to the individual who is the subject of the information and
- Disclosures to HHS to determine compliance with the regulation.

What uses and disclosures require an individual's consent?

A health care provider in a direct treatment relationship with an individual must obtain the consent of the individual to use or disclosure protected health information for treatment, payment, or health care operations. An individual may request a restriction on how protected health information is used or disclosed for treatment, payment, or health care operations.

Consent is not required for a health care provider in an indirect treatment relationship (e.g., a radiologist who reviews a patient's x-rays and discloses a report to a consulting physician).

What uses and disclosures require an individual's authorization?

Individual authorization is required for most uses or disclosures other than for treatment, payment, or health care operations.

What uses and disclosures are permitted without an individual's consent or authorization?

As a practical matter, it is sometimes necessary to strike a balance between individual privacy rights and public good. To do this, the privacy rule enumerates a specific set of activities for which the public benefits are sufficiently important to warrant limited disclosure of protected health information without an individual's consent or authorization.

For each of these activities, uses and disclosures are permitted—but not required. For each activity, the privacy rule designates the specific conditions under which the use or disclosure can occur. In each case, the specific conditions are tailored to the particular purpose.

The particular activities enumerated in the rule include the following:
- Those required by law;
- Specific public health activities authorized by law (this is discussed in more detail below);
- Abuse, neglect, or domestic violence reporting;
- Health oversight activities authorized by law;
- Judicial and administrative proceedings;
- Law enforcement;
- Identification of deceased persons or cause of death by medical examiners or coroners;
- Organ, eye, or tissue donation;
- Research, with approved waiver;
- Averting serious threats to health or safety;
- Activities related to national defense and security;
- Government programs providing public benefits; and
- Compliance with workers' compensation law.

For example, reporting adverse events or product defects to manufacturers under the jurisdiction of the Food and Drug Administration is a permitted disclosure because protecting patients from unsafe products is an essential public responsibility authorized by law. Reporting adverse events or product defects requires protected health information, and the benefit accrues beyond the individual to society as a whole. Individual consent or authorization is not required for such disclosures.

What kind of health information is not protected?

De-identified information is not protected information under the privacy rules.

In a sense, the privacy rules establish incentives for information to be de-identified. Identifiable information can be used and disclosed only according to a set of complex rules, whereas de-identified information can be used and disclosed freely. Since identifiable information is not necessary for many purposes, these rules should provide an incentive to make greater use of de-identified information.

How can information be de-identified?

The privacy rules specify two methods for de-identification.

One method requires a formal disclosure analysis to be performed by a professional with expertise in the appropriate statistical techniques. Information is deemed to be de-identified if the disclosure analysis concludes that the risk of identification is very small, with appropriate documentation of the methods and results that support such a determination.

The second method might be termed "de-identification by elimination." The rules designate a list of elements that, if all are removed, produce de-identified health information. Information de-identified in this manner can then be disclosed unless the covered entity knows that the remaining information could be used alone or in combination with other information to identify an individual.

The elements to remove include: names; geographic subdivisions smaller than a State; all elements of dates smaller than a year; telephone and fax numbers; Social Security, medical record, health plan identification, and account numbers; certificate/license numbers; vehicle identification, serial, and license plate numbers; Internet addresses (URLs, IPs, e-mail); biometric identifiers (finger and voice prints); certain photographic images; and any other unique identifying number, characteristic, or code. This method applies to identifiers not only of the individual but also of the individual's relatives, employers, and household members.

Can protected health information ever be disclosed for research?

Yes, identifiable information can be disclosed without individual authorization for research under limited conditions. This recognizes the value of research and the fact that individually identifiable information is sometimes essential to such research.

A waiver from a properly constituted Institutional Review Board (IRB) or privacy board is required for such disclosures. The IRB or privacy board must apply specific criteria before making a waiver determination.

The criteria for a waiver include the following:
- The use or disclosure involves no more than minimal risk to the individuals.
- The waiver will not adversely affect the privacy rights and welfare of the individuals.
- The research could not practicably be conducted without access to the protected health information.
- The privacy risks are reasonable when balanced against the potential benefits and expected advantages of the research.
- There is an adequate plan to protect individual identifiers and to destroy the identifiers at the earliest possible opportunity.
- There is adequate written assurance that the protected information will not be reused inappropriately.

An alternative method of providing access to protected health information for research is called "reviews preparatory to research." Again, the protected health information must be necessary for the research. Under this method, a covered entity permits researcher access to protected information onsite as necessary to prepare a research protocol or for other purposes preparatory to research, and no protected health information is removed from the covered entity by the researcher.

What individual rights are conferred by the privacy rules?

Greater consumer control over sensitive health information was one of the principles expressed in the HHS recommendations for Federal privacy legislation. This principle was then incorporated into the privacy regulations.

Consumer control is expressed as a set of rights of an individual:
- To inspect and copy their protected health information,
- To obtain a record of certain disclosures,
- To amend or correct protected health information,
- To consent before information is released,
- To request certain restrictions on uses and disclosures,
- To receive written notice of information practices from health plans and providers, and
- To complain to the covered entity or HHS.

What is the relationship of these privacy regulations to other law?

HIPAA privacy rules do not automatically preempt (replace) all other privacy law.

These national privacy rules do not preempt the following:

- More stringent State privacy laws,
- State requirements for public health reporting, or
- State laws regulating health plans.

A State law is defined as "more stringent" if it places greater restrictions on permitted uses and disclosures or provides greater privacy protections (e.g., narrows the scope of authorizations or consent) or provides greater individual rights. States are free to enact more stringent privacy protections.

These exceptions to preemption are designated in the HIPAA statute. Other State law exceptions to preemption may be requested and approved by HHS.

The HIPAA privacy rules preempt contrary State law. A State law is defined as "contrary" if it would be impossible to comply with both State and Federal requirements or if the State law stands as an obstacle to achieving HIPAA's purpose.

In general, HIPAA privacy rules interact compatibly with other Federal law, including, for example:

- The Privacy Act of 1974,
- The Freedom of Information Act,
- The Common Rule for protection of human subjects in biomedical research, 45 CFR 46A-D, and
- Federal Substance Abuse Confidentiality Regulations, 42 CFR Part 2.

acy and DAWN

Does DAWN collect protected health information?

Yes, DAWN collects some protected health information. DAWN collects date and time of ED visit and patient ZIP Code. Under the privacy rules for de-identification by elimination (discussed earlier), these constitute protected health information. However, DAWN does not collect direct patient identifiers, such as medical record number or patient name.

Does DAWN request the minimum amount of information necessary to fulfill its purpose?

According to an external assessment of DAWN's design, DAWN collects less than the minimum amount of information necessary to fulfill its purpose. Plans are underway to redesign DAWN in order to improve its usefulness. These plans would add to the information collected on DAWN cases. However, there are no plans to collect additional patient identifiers.

What provision in the privacy rule permits disclosure of protected health information to DAWN?

Disclosures for DAWN fall under disclosures for public health activities authorized by law, 45 CFR 164.512(b)(1). These disclosures are permitted without individual consent or authorization.

The privacy rules permit disclosures to a public health authority authorized by law to collect or receive information for preventing or controlling disease, injury, or disability and for the conduct of public health surveillance, investigations, and interventions.

"Disclosure of protected health information to DAWN is permitted under the Federal privacy standards § 164.512(b)(1) uses and disclosures for public health activities."

SAMHSA is a public health authority required by law—Section 505 of the Public Health Service Act (42 U.S.C. 290aa-4)—to collect data on:

- The number of individuals admitted to the emergency rooms of hospitals as a result of the abuse of alcohol or other drugs and
- The number of deaths occurring as a result of substance abuse, as indicated in reports by coroners.

Does the privacy rule require hospitals to disclose protected health information to DAWN?

The privacy rule specifies the conditions under which such disclosures are permitted. There is no requirement, however, for hospitals to participate in DAWN or to disclose protected health information to DAWN.

What are the restrictions on the use or disclosure of protected health information after it is disclosed to DAWN?

Federal law enacted in October 2000 restricts the uses and disclosures of data collected by DAWN. Section 501(n) of the Public Health Service Act (42 U.S.C. 290aa) states (emphasis added):

> Section 501(n) LIMITATION ON THE USE OF CERTAIN INFORMATION. No information, if an establishment or person supplying the information or described in it is identifiable … may be used for any purpose other than the purpose for which it was supplied unless such establishment or person has consented … to its use for such other purpose. Such information may not be published or released in other form if the person who supplied the information or who is described in it is identifiable unless such person has consented … to its publication or release in other form.

How are these restrictions implemented to prevent misuse of protected health information in DAWN?

OAS/SAMHSA has developed the following policies and procedures to prevent misuse or disclosure of protected health information in DAWN:

- Employees of OAS/SAMHSA and its contractors sign confidentiality agreements that spell out the confidentiality requirements, how those requirements affect employees' behavior and use of data, and the penalties associated with violations.

  DAWN field liaisons and regional coordinators are subject to these policies and procedures because they are employees of OAS/SAMHSA's contractors.

- Every individual affiliated with DAWN at SAMHSA and its contractors receives specific training on the confidentiality and data protection rules that apply to DAWN.

- Public use data files contain only de-identified data. Users of public use data files sign data use agreements that delineate the purposes for which the de-identified data can be used and the penalties for misuse.

- Certain data elements—date and time of visit and patient ZIP Code—are available only to authorized employees of SAMHSA and its contractors. These data elements are stripped to create de-identified files.

- Tabulations of DAWN data are reviewed for confidentiality risks before release. Suppression rules are applied to small cells to minimize the risk of inadvertently disclosing the identity of an individual or a hospital.

"No identifiable information in DAWN may be used for any purpose other than the purpose for which it was supplied, without consent (42 U.S.C. 290aa)."

What policies and procedures apply to DAWN reporters?

DAWN reporters access hospital records for the purpose of abstracting DAWN data elements. DAWN reporters perform this function onsite with the approval of the participating hospital.

A DAWN reporter may be:

- An employee of the participating hospital whose use of protected information to abstract DAWN elements is authorized by the hospital.

- A business associate of a participating hospital engaged to perform the DAWN reporting function on behalf of the hospital. A business associate contract would restrict the associate's use of protected information and the disclosure of data elements to DAWN.

- A contractor of OAS/SAMHSA subject to all the policies, procedures, and training applicable to DAWN contractors.

or More Information about HIPAA

Where can I get more information about the HIPAA privacy rules?

This report is a very brief overview of some of the major HIPAA requirements with a concentration on those that relate to DAWN. However, it is a summary and not intended to be comprehensive.

You should not rely on this report alone to plan for HIPAA compliance. You should begin by reading the privacy rules and consulting with in-house counsel.

The privacy regulation consists of several parts. The "preamble" to the regulation includes the following:

- Background,
- An expanded explication of the major provisions,
- Responses to comments received on the proposed rule, and
- A final impact analysis.

The "meat" of the regulation is the actual regulation text, which becomes part of the Code of Federal Regulations, 45 CFR Parts 160 and 164.

The regulation text exactly as it appeared in the *Federal Register* on December 28, 2000 (the regulation text begins on *Federal Register* page 82798) is available online in Adobe™ Acrobat™ portable document format in:
http://aspe.hhs.gov/admnsimp/final/PvcFR07.pdf
and in:
http://aspe.hhs.gov/admnsimp/final/PvcFR08.pdf.

The regulation text is available online in a more easily readable format at:
http://aspe.hhs.gov/admnsimp/final/PvcTXT01.htm.

The HHS Office for Civil Rights (OCR) has been designated as the agency responsible for implementing and enforcing the privacy rules. The OCR privacy web page is: *http://www.hhs.gov/ocr/hipaa/*.

Where can I get more information on Administrative Simplification?

The official HHS Administrative Simplification web site is: *http://aspe.hhs.gov/admnsimp/*.

This site includes the following:

- Frequently asked questions,
- Copies of the HIPAA statute and regulations to view online or download,
- Public comments on proposed rules,
- Implementation Guides for HIPAA electronic transactions,
- Links to other HIPAA-related web sites, and
- Instructions for subscribing to the HIPAA-REGS listserv. Subscribers receive e-mail notifications of major HIPAA actions.