How does HIPAA affect public health reporting?

Doug Campos-Outcalt, MD, MPA
University of Arizona Department of Family and Community Medicine, Phoenix

Since the Health Insurance Portability and Accountability Act (HIPAA) privacy rule was put into effect in April 2003, health-care providers have sometimes been confused about what information they can legally disclose to public health agencies. A clear understanding of permissible disclosure will enable family physicians to continue their important role of providing individual patient information for the critical activities of disease surveillance, outbreak investigation, monitoring causes of death and birth complications, assuring health care services, conducting public health research, and formulating health policy.

HIPAA DOES NOT PROHIBIT DISCLOSURE FOR PUBLIC HEALTH PURPOSES

The HIPAA is intended to protect the public from unauthorized access to, use of, and disclosure of individually identifiable health information. It places responsibility on health care providers to avoid using or disclosing protected health information (PHI) unless authorized by the person to whom it pertains, or unless the disclosure or use is required or permitted by regulation or law. Specifically excluded from the requirement for individual authorization are disclosures for public health activities. This means that sharing PHI for public health purposes is permitted as long as the agency to which the information is provided is legally authorized to collect and receive the information (see **Lawful recipients of personal health information**).

This specific exclusion was allowed because public health authorities have a legitimate need for PHI to ensure public health and safety, and because public health agencies have a track record of protecting the confidentiality of PHI. The HIPAA privacy rule attempts to strike a balance between individual privacy rights and the need for public protection.

LAWFUL DISCLOSURE: EXAMPLES

It's instructive to consider how this public health HIPAA exception plays out in the daily practice of medicine. First, some definitions:

Protected Health Information. Individually identifiable health information transmitted electronically or any other way. It includes information about past, present, or anticipated mental or physical health, and the provision of or payment for health care.

Covered entities. These are the entities who must adhere to the HIPAA rules. Included are health care providers, health plans, and health

Correspondence: 4001 North Third #415, Phoenix, AZ 85012. E-mail: dougco@u.arizona.edu.

Lawful recipients of personal health information

Public health agencies included in this category include state, territorial, tribal, and local health departments, as well as federal health agencies such as the Centers for Disease Control and Prevention, the Food and Drug Administration, the National Institutes of Health, the Occupational Safety and Health Administration, the Substance Abuse and Mental Health Services Administration, and others. It also includes individuals and agencies working under a grant of authority from a public health agency.

care clearinghouses that transmit any health information in an electronic format.

Personal Identifiers. Information that can be used to find the identity of an individual to link them to their PHI.

Scenario 1

A family physician's patient dies at home. The physician is asked to fill out a death certificate, which contains PHI as defined by the HIPAA privacy rule. Is this permitted without family authorization?

Unauthorized disclosure is permitted. Vital statistics—required information on death and birth certificates—has not been changed by HIPAA. The information required on the death certificate can be provided without authorization.

Scenario 2

A patient is diagnosed with tuberculosis. This is a reportable disease per the state health code. Can the physician report the PHI requested on the disease reporting form?

Unauthorized disclosure is permitted. Each state health authority requires health care providers to report information about individuals who have contracted a disease of public health significance. Reportable disease lists differ by jurisdiction, and physicians should be aware of the diseases reportable in their areas and how the information is to be reported. Individual authorization for release of PHI in these disease reports is not required by HIPAA.

Scenario 3

A physician examines an infant who has unexplained injuries. Child abuse is suspected. Is child abuse reporting exempted from the privacy rule?

Unauthorized disclosure is permitted. Reporting of child abuse and neglect is exempted. This information may even be reported to a non-health agency, such as a child protective service, as long as the reportable information is required by law, and individual authorization is not required.

Scenario 4

A patient suffers what appears to be an adverse reaction to a medication. The FDA adverse event reporting form asks for PHI. Can a physician report PHI in this instance without patient authorization?

Unauthorized disclosure is permitted. Reporting of adverse events or reactions from drugs, food, biological products, and medical devices is still permitted without authorization.

Scenario 5

A patient is newly diagnosed with lung cancer. The state maintains a cancer registry and physicians are required to report PHI about patients with cancer. In this state the cancer registry is maintained by the university under contract with the State Health Department. Is reporting permitted without patient authorization?

Unauthorized disclosure is permitted. Cancer and immunization registry reporting of PHI is still permitted even if the entity responsible for the registry is not a public health agency, as long as it is under the authority of the agency to perform this public health function.

Scenario 6

A patient dies from meningitis and the local health department requests to view the hospital record to investigate cause of death. The cause turns out to be West Nile virus, which is not on the list of reportable diseases. Is the health department permitted to view the record and is authorization required?

Unauthorized disclosure is permitted. The privacy rule exception does not require a law or regulation specifically mandating disclosure. The health care provider can release requested information to a public health authority when the information is for the purpose of controlling disease, injury, or disability. The information released should be the minimum necessary for the stated public health purpose, and the provider can rely on the agency to determine what that information is. In this case, examination of the record is permitted and authorization is not required.

Scenario 7

An auditor from the Vaccine for Children program arrives at the office and requests to see patient records to audit adherence to the rules governing this program. Is the auditor allowed to exam records, and is authorization required?

Unauthorized disclosure is permitted. Patient records can be reviewed by staff of public health agencies authorized by law to collect PHI for program management purposes. No patient authorization is required.

Scenario 8

A local community agency is concerned about the potential health effects of groundwater contamination. They request information about all your patients who have contracted cancer within the past 5 years. What information can you provide them?

PHI disclosure requires patient authorization. This agency, unless under the authority of a public health agency to collect PHI, cannot obtain PHI without patient authorization. However, de-identified information could be provided. De-identified data are not covered by HIPAA and do not require individual privacy protection or authorization for release. De-identification means removing 18 "identifiers" (**Table**) or enough information that allows a statistician to conclude that the chance of an individual being identified is remote.

PHYSICIAN OBLIGATIONS WITH DISCLOSURE

Confirm the legitimacy of a request. Even though physicians can release PHI to public health agencies without a patient's authorization, they have other obligations to meet. One of these is to ensure that the person or agency requesting PHI is a legitimate public health authority. If the request is made in person, some form of credentials or proof of government status should be provided. If the request is in writing, it should be on official letterhead. A person or agency acting under the authority of a pubic health agency should provide proof of this authority. If physicians have any doubt about the authenticity of a request, they should call the agency being represented and inquire.

Let patients know. The second obligation is to provide information about the disclosure to the individual whose PHI was released, if this information is requested, and to inform patients in statements about privacy practices that PHI information is released to public health agencies when required and permitted by law.

OTHER EXCEPTIONS TO HIPAA

HIPAA allows the legitimate use of PHI, without authorization, for the purpose of protecting the public under conditions involving law enforcement, court proceedings, worker's compensation, and national security. These exceptions are outside the scope of this article.

EXPLAIN HIPAA TO PATIENTS

The trend toward electronic medical records and the increasing public concern about privacy

TABLE

Individual identifiers to be removed from reports

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.

- Names
- All geographic subdivisions smaller than a state, including county, city, street address, precinct, zip code (first 3 digits OK if geographic unit contains >20,000 persons), 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
- 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: "HIPAA privacy rule and public health," *Morbidity and Mortality Weekly Report*, April 11, 2003; 52:1–12.

led to the enactment of the HIPAA privacy rule. A natural tension exists between individual rights and public protection, and the HIPAA privacy rule attempts to balance these competing concerns. For patients who are concerned about confidentiality, family physicians can explain the purpose of public health exceptions and give reassurance about how public health agencies have a good record of protecting individuals' identity.