Patient Anonymity (2001 update)

Save to myBoK

This practice brief has been retired. It is made available for historical purposes only.

Editor's note: The following information supplants information contained in the November/December 1997 "Patient Anonymity" practice brief.

Background

Section 2, Paragraph 4 of The Privacy Act of 1974 (Public Law 93-579) states, "The right to privacy is a personal and fundamental right protected by the Constitution of the United States."[1] Even though the words "right to privacy" do not specifically appear anywhere in the US Constitution, a number of constitutional scholars concur that the right to privacy is implied in the document. Through the evolution of common law, the status of individual privacy has evolved from a privilege to a right.

This right to privacy continues to evolve. Each new advance in information technology heightens society's expectation that individual privacy should be actively protected. For example, not long ago, many local newspapers published the names of all patients admitted to local hospitals. Over time, society has changed its view of the practice of openly revealing patient admission information. This view, reinforced by numerous accounts of negative and damaging experiences involving breaches of patient privacy, has induced many facilities to subscribe to policies that strictly protect patient anonymity.

Today, many patients are seeking control of their personal health information. This change in public opinion is a response to the increasing number of entities seeking access to identifiable patient information, as well as the increasing speed and volume at which information can be transmitted.

The Impact of HIPAA's Privacy Rule

In the Health Insurance Portability and Accountability Act's final privacy rule (45 CFR, parts 160 through 164), the federal government requires covered entities to provide individuals with a notice of information practices and to obtain a written consent from the individual for use and disclosure of the information for treatment, payment, and healthcare operations. Generally speaking, unless an information practice is addressed in the notice and consent obtained, use or disclosure would require a specific authorization. Of interest, however, are a few exceptions.

Use and Disclosure for Directory Purposes

The final privacy rule allows a covered entity to use or disclose protected health information for directory purposes without the individual's written consent or authorization, provided the individual was informed of the intended use or disclosure in advance and had the opportunity to either agree to or prohibit the use or disclosure. Furthermore, the rule allows the covered entity the option to inform and obtain the individual's objection or agreement orally.

The covered entity may disclose for directory purposes the individual's name, location within the facility, and condition in general terms that do not communicate specific information. This information may be provided to clergy and persons who ask for the individual by name. Clergy may also be provided with the individual's religious affiliation.

Should a patient object to having his or her protected health information used or disclosed for directory purposes, a mechanism must exist to prevent placement of the information in the public directory and its subsequent disclosure.

If the opportunity to object cannot practicably be provided because of an individual's incapacity or an emergency treatment circumstance, a covered provider may use or disclose some or all of the directory information if such disclosure is consistent

with a prior expressed preference and in the individual's best interest. The covered provider must inform the individual and provide an opportunity to object when it becomes practicable to do so.

Use and Disclosure to Family and Close Personal Friends

Similarly, covered entities may also disclose to an individual's family, close personal friends, or other persons identified by the individual protected health information without prior written consent or written authorization if the covered entity obtains the individual's agreement and provides the individual with the opportunity to object, or if the covered entity reasonably infers from the circumstances that the individual does not object to the disclosure.

If the individual is not present or does not have the opportunity to agree or object to the use or disclosure because of incapacity or an emergency circumstance, the covered entity may determine whether the disclosure is in the best interest of the individual and if so, disclose only the information that is directly relevant to the person's involvement with the individual's care.

Use and Disclosure for Notification Purposes

The covered entity may also use or disclose protected health information to notify or assist in the notification of a family member, a personal representative, or another person responsible for the care of the individual as to the individual's location, general condition, or death. This disclosure may take place if the covered entity obtains the individual's agreement and provides the individual with the opportunity to object to the disclosure (and the individual does not express an objection) or the covered entity reasonably infers from the circumstances that the individual does not object to the disclosure.

If the individual is not present or does not have the opportunity to agree or object to the use or disclosure for notification because of incapacity or an emergency circumstance, the covered entity may determine whether the disclosure is in the best interest of the individual and, if so, disclose only the protected information that is directly relevant to the person's involvement with the individual's care.

A covered entity may also use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts for the purpose of coordinating notification.

Other Uses and Disclosures Required by Law

Covered entities may use or disclose protected health information to the extent that such use or disclosure is required by law and the disclosure complies with and is limited to the relevant requirements. Covered entities may make such disclosures to organizations such as:

- **public health authorities** authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, disability, or recording vital events such as birth or death
- **health oversight agencies** for activities authorized by law
- **individuals exposed to a communicable disease** or who may otherwise be at risk of contracting or spreading a disease or condition if the covered entity or public health authority is authorized by law to notify such person
- **employers responsible for workplace medical surveillance** to record illness or injury or to carry out responsibilities for workplace medical surveillance (in order to comply with its obligations under 29 CFR parts 1904 through 1928 and 30 CR parts 50 through 90 or under state law having a similar purpose). In this case, however, the covered entity must provide the individual with a copy of the notice of information practices or have it posted in a prominent place where care is provided
- **public health or government authorities** for law enforcement purposes. For example, information may be disclosed for use in reports of abuse, neglect, or domestic violence or as required by laws that require the reporting of certain types of wounds or other physical injuries. Furthermore, entities may disclose information in compliance with the requirements of a valid court order, warrant, subpoena, or summons, as well as in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person or about an individual who is or is suspected to be a victim of a crime
- **coroners, medical examiners, and funeral directors** for the purpose of identifying a deceased person, determining a cause of death, or duties as authorized by law

- **organ procurement organizations** or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating donation and transplantation

State Laws

Many states have legislation or regulation about the use and disclosure of health information, including information that may be released without an individual's consent.

The HIPAA privacy final rule preempts state laws, except where state law is more stringent or where an exception is granted by the secretary of the Department of Health and Human Services.

Recommendations

Organizations will need to develop policies and mechanisms compliant with federal and state laws that allow the patient to control, to the extent possible, the amount and type of protected information released.

Because the process of determining the more stringent federal or state law is complex, seek the advice of legal counsel in originating or finalizing such policies and procedures.

Remember that the underlying axiom of a patient anonymity policy should be that, as one industry publication puts it, "the patient has the option to expressly state that he or she does not want any information, including confirmation of his/her presence in the facility, released."[2] This is true with the exception of disclosures required by law.

Designating a Spokesperson

Your facility policy should specify exactly who is authorized to assign patient anonymity. Establish a mechanism to immediately notify key staff involved in protecting patient anonymity (e.g., security, public relations, or administration) each time anonymity is provided to a patient.

The HIPAA final privacy rule requires a covered entity to designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity. This designated privacy official is one possible candidate for the responsibility of managing patient anonymity.

Designate a spokesperson to address any inquiries received from the media or other authorities. Weekend and evening coverage for the spokesperson should also be provided. An individual experienced in healthcare public relations would be good choice for the spokesperson position. If such a person is unavailable, the chosen staff member should be someone with excellent public speaking ability and strong communication skills.

A spokesperson should never release information that would embarrass a patient. In situations where there is a known potential risk of danger to the patient should his/her location be revealed, the spokesperson should not release any information or confirmation of the patient's presence.

Procedures should ensure that any information approved for release is consistent and accurate. Once anonymity status has been assigned, no information regarding the patient's presence in the facility or condition should be released without the patient's authorization.

Expect that employees may be approached by individuals outside the organization seeking information on patients. The best defense to this type of tactic is regularly scheduled employee education coupled with strong, well-written policies that are widely distributed to all employees, volunteers, and contractors.

Only a patient's physician should make statements regarding diagnosis or prognosis. The spokesperson should use the following one-word condition descriptions when releasing information about the patient:

Undetermined: Patient awaiting physician and assessment

Good: Vital signs are stable and within normal limits. Patient is conscious and comfortable. Indicators are excellent

Fair: Vital signs are stable and within normal limits. Patient is conscious, but may be uncomfortable. Indicators are favorable

Serious: Vital signs may be unstable and not within normal limits. Patient is acutely ill. Indicators are questionable

Critical: Vital signs are unstable and not within normal limits. Patient may be unconscious. Indicators are unfavorable

"Stable" should not be used as a condition. Furthermore, this term should not be used in combination with other conditions, which by definition often indicate a patient is unstable.[3]

Following review and written approval by the patient, a more explicit statement could be released should the patient believe a detailed statement is appropriate under the circumstances.

In situations where the news media is seeking access to health information that the patient has refused to release, the burden of compelling the health provider to release information should be on the news media unless disclosure is otherwise required by law.

Protecting Against Threats to Patient Privacy

Special procedures for handling the patient records of individuals who request anonymity can be developed. Among the steps that can be taken to protect unauthorized disclosures are:

- omitting the patient's name from the cover of the record
- using an alphanumeric code or alias name in place of the patient's real name. One format used is a combination of the patient's initials and business office account number. Use of an alias name such as John Doe for all patients can be confusing, especially if more than one John Doe is registered at a time
- replacing the patient's name with an alphanumeric code or alias name on all "bed boards," bulletin boards, and patient room signs
- restricting computer system access to those users who need to know the patient's identity to perform their jobs
- placing a warning message on the access screens of all patients that request anonymity. The warning should remind the user that they are about to access a restricted file and that security audits are performed at the facility
- designating one individual responsible for controlling access to the restricted medical record in facilities with paper record systems. The record should be maintained in a secure area when it is not being used by a healthcare provider
- employing a mechanism that will lock out a user that attempts to access information beyond his/her security clearance with repeated use of an improper code
- performing periodic audits to ensure that the organization's policies are being followed and are still effective
- employing mechanisms that will alert the facility security officer when a system user attempts to access information beyond his or her security clearance
- developing written policies outlining access to patient information
- providing employees, medical staff members, students, and volunteers with specific training about their responsibility to protect confidentiality of patient health information
- requiring that at the time of employment all staff members, students, and volunteers are required to sign a nondisclosure agreement. Organizational policy should require an annual review of confidentiality policies with acknowledgement
- upon discharge, limiting access to the record during the chart completion process to designated employees with a valid need to know
- once the chart is completed, placing it in a secure file that is accessible only to the director of health information management and other designated staff members. Charts should not be made available for research or reviews unless a special release is obtained first
- at discharge, placing the patient's actual name in the master patient index with a crosswalk software application to the alias

Prior to developing policies and procedures, the facility should carefully review all applicable state laws addressing the release of identifiable patient information.

Notes

1. The Privacy Protection Study Commission. *The Privacy Act of 1974: an Assessment.* Washington, DC: 1977, Appendix 4.

2. Society for Healthcare Strategy and Market Development. *General Guide for the Release of Information on the Condition of Patients*. Chicago, IL: 1997.

3. Ibid.

References

"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 65, no. 250 (December 28, 2000). Available at http://aspe.hhs.gov/admnsimp/.

Douglass, Kara. "Inside Track: Madonna Slept Here." *Hospitals and Health Networks* no. 14 (1997): 61.

Goldman, Janlori, and Mulligan, Deirdre. *Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality*. Washington, DC: The Center for Democracy & Technology, 1996.

Health Law Center, Hospital Law Manual, Administrator's Volume. Aspen Publishers, Inc., Volume 1B, Section 3-19, 1995, pp. 51-55.

Lewton, Kathleen L. *Public Relations in Health Care: A Guide for Professionals*. Chicago, IL: American Hospital Publishing, Inc., 1995.

Privacy Protection Study Commission. *The Privacy Act of 1974: an Assessment.* Washington, DC: Superintendent of Documents, US Government Printing Office, 1977.

"Protecting the Privacy of the Rich and Famous." *Medical Record Briefing* 12, no. 7 (1997): pp. 4-5.

Roach, William H. "Legal Review: Coping with Celebrity Patients." *Topics In Health Record Management* 12, no. 2 (1991):67-72.

Roach, William H. *Medical Records and the Law*. Gaithersburg, MD: Aspen Publishers, 1994.

Rowland, Howard S., and Rowland, Beatrice L. *Hospital Legal Forms, Checklists, & Guidelines*. Volume 2. Gaithersburg, MD: Aspen Publishing Co., 1997.

Society for Healthcare Strategy and Market Development. *General Guide for the Release of Information on the Condition of Patients*. Chicago, IL, American Hospital Association, 1997.

Prepared by

Harry B. Rhodes, MBA, RHIA, director of HIM products and services

Acknowledgments

Jill Callahan Dennis, JD, RHIA
Gwen Hughes, RHIA

This article is based on the privacy rule issued on December 28, 2000. At press time the rule was under review by the new administration and could be subject to change.

Article citation:
Rhodes, Harry. "Patient Anonymity (Updated) (AHIMA Practice Brief)." *Journal of AHIMA* 72, no.5 (2001): 64O-R.