Release of Information for Marketing Purposes (1998)

Save to myBoK

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

Background

The growing computerization of health information is increasing both the supply of and demand for health data. Today, with so many requests for information, HIM professionals must know how to handle each type of request. Both internal and external health information requests for marketing purposes are now surfacing frequently. There is a significant demand for health data about individuals for use in direct marketing. An example of external use includes medical and surgical suppliers and pharmaceutical companies that want to identify potential customers. These vendors will look to marketing companies that compile and sell lists of individuals' names. Internally, patient data might be used to identify potential contributors for a new facility (e.g., a cardiac patient is contacted for a contribution to the construction of a new coronary care unit). Another internal request for patient data might be for the marketing of healthcare services that the facility offers. These lists may select individuals by a variety of ailments or other criteria that fit into specific categories of particular service needs.

As seasoned consumers, the majority of us have simply accepted mass marketing invasions into our lives. However, those who are unwilling to accept marketing's intrusion into their private lives have responded by simply refusing to supply the information. Refusal to complete information-seeking instruments such as product warranty cards, sweepstakes entry forms, and preferred customer cards is just one action taken to cut off the supply of information needed by marketing enterprises.

Data contained in a patient's health information record cannot be compared to the information collected on product warranty cards or sweepstakes entry forms. Once revealed, health information can be damaging to a patient's professional and personal lives, not to mention embarrassing. Healthcare professionals have a responsibility not to reveal -- without consent -- information obtained while caring for a patient. Hospitals, nurses, HIM professionals, physicians, therapists, and other healthcare workers risk being sued for invasion of privacy if confidential information from a patient's health record (or any information procured during patient care) is released inappropriately.

Confidential Information vs. Nonconfidential Information

When faced with any request for the release of information, it is important to remember what is considered confidential information versus nonconfidential information. Confidential information is made available during the course of a confidential relationship between the patient and healthcare professionals. Confidential information includes, but is not limited to, all clinical data, plus the patient's address upon discharge if it is different from the address given during admission. Disclosure of any health information relating to alcohol or drug abuse is governed by specific federal statutes codified in 42 CFR, Ch.1, Part 2 (1983). Disclosure of information pertaining to mental health and other sensitive conditions may be restricted by law in some states.

Nonconfidential information is that which is generally common knowledge. It requires no specific request by the patient to restrict disclosure. Nonconfidential information includes the following:

- Name of patient
- Verification of hospitalization or outpatient services
- Date of services

Secondary Use of Health Information

The health record has become a rich repository of information for people and institutions that are not directly involved in the health treatment and payment process. The growing demand for, and supply of, health information for uses that are far

removed from the health treatment and payment process make it imperative to establish a system of controls for identifiable health information that limits the unrestricted spread of that information. It is important to keep in mind the basic principles of disclosure of health information when handling requests for information not directly related to the continuum of care. Remember that health records (regardless of the media on which they are maintained) are the property of the healthcare provider, but the health information itself belongs to the patient. Disclosure of health information must be done prudently to protect the patient's right to privacy.

In recognition of the widespread increase in the secondary uses of health information, Secretary of Health and Human Services Donna Shalala made recommendations to Congress on September 11, 1997, regarding security of health information. Some of the recommendations apply to release of information:

- Patient-identifiable information should not be disclosed except as authorized by the patient or as explicitly permitted by the legislation
- Patient information should be used within an organization only for purposes reasonably related to the purposes for which the information was collected
- A provider or payer should not be allowed to condition, treatment, payment, or coverage on a patient's agreement to disclose health information unless the information is needed for treatment, coverage, or payment purposes
- All disclosures of identifiable information should be limited to the minimum necessary to accomplish the purpose of the disclosure

Shalala also made recommendations to Congress concerning limitations on the use of health information:

- Providers and payers should be permitted to use the health information only for purposes compatible with and directly related to the purposes for which the information was collected or received, or for purposes for which they would be authorized to disclose the information. For example, a provider should be able to use identifiable health information for mailing reminders to patients to schedule appointments. It should not be able, absent patient consent, to make available its patient list to a health company for use in a direct mailing announcing a new product or service (even if that product or service might benefit the patient)
- The fact that an organizational entity holds information is not a proper basis for its uncontrolled use within the organization or outside of the organization. Entities holding information should have to make distinct and explicit choices about which activities are sufficiently connected with their health activities to warrant the use of identifiable health information. Other uses could be made only with patient authorization, or under provisions of the legislation that permit disclosure without patient authorization

The report "For the Record: Protecting Electronic Health Information," which was released by the National Research Council, has made recommendations that address actions to protect the privacy and security of health information held by individual healthcare organizations. The committee recommends "a national debate to determine how and to what extent greater control needs to be taken to address the privacy concerns that result from the legitimate and widespread systemic flows of information within the healthcare system. Only when this national debate takes place can policy be formulated properly."

This report also recommends that "organizations that collect, analyze, or disseminate health information should adopt a set of fair information practices similar to those contained in the federal Privacy Act of 1974. These practices would define the obligations and responsibilities of organizations that collect, analyze, or store health information; give patients the right to demand enforcement of these obligations and responsibilities; and require disclosure of data collection activities to make the sharing of health information more transparent to patients. Such disclosure would educate patients about the flows of health data and their rights in controlling those flows, thereby facilitating the discussion of privacy and security issues and the development of consensus. The report states that personal awareness of privacy rights and potential abuses is one of the best countervailing pressures against the economic incentives that drive organizations to share information. Moreover, public awareness and concern may be an essential prerequisite to the passage of necessary legislation of any strength."

Recommendations for Handling Marketing Requests

- Review existing release of information policies. Do they cover the handling of marketing requests for information?
- Establish ownership for the release of health information for marketing purposes. Decide who is responsible for this process
- Develop a policy addressing access to patient information for internal and external marketing purposes. One possible approach to developing a policy would be to enlist the expertise of the institutional review board. If your facility does not have an institutional review board, identify the committee responsible for approving or disapproving marketing requests, such as the HIM or medical records committee
- Protect the identity of patients and providers. Patient identifiers can be derived from a variety of data elements. Data, singular or in combination, that may allow a patient to be identified include: name, medical record number, social security number, date of birth, gender, marital status, occupation, employer, address, phone number, and any unique and identifying physical characteristics
- Educate staff on the issues surrounding the secondary use of health information and make them aware of their responsibilities regarding the release of health information
- Be proactive or involved in decision making at your healthcare facility to know how patient information is being used
- Stay current on changes in accrediting body standards, federal regulations, and state laws

References

Abdelhak, Mervat, Sara Grostik, Mary Alice Hanken, and Ellen Jacobs, eds. *Health Information: Management of a Strategic Resource*. Philadelphia, PA: W.B. Saunders Co., 1996.

Brandt, Mary. *Maintenance, Disclosure, and Redisclosure of Health Information*. Chicago, IL: AHIMA, 1995.

Fuller, Sandra. *Security and Access: Guidelines for Managing Electronic Patient Information*. Chicago, IL: AHIMA, 1997.

House Committee on Government Operations, *Health Security Act*, 103rd Cong., 2d sess., 1994, H. Rept. 3600, 72-75.

National Information Infrastructure and National Research Council. *For the Record: Protecting Health Information*. Washington, DC: National Academy Press, 1997.

US House. 1994. *Health Security Act* Report no. 13-601, Part 5, 103rd Cong., 2d sess.

US Senate. 1997. Hearing before the Senate Labor and Human Resources Committee. Testimony of Donna Shalala, Secretary of Health and Human Services. 105th Cong., 1st sess., 11 September.

Prepared by

Julie J. Welch, RRA, HIM practice associate

Acknowledgments

The assistance from the following individuals is gratefully acknowledged:
Jennifer Carpenter, RRA
Kathleen Frawley, JD, MS, RRA
Donna Fletcher, MPA, RRA
Sandra Fuller, MA, RRA
Harry Rhodes, MBA, RRA

Issued: January 1998

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.