HIPAA Reins in Shadow Charts, Independent Databases (HIPAA on the Job)

by Margret Amatayakul, RHIA, CHPS, FHIMSS

Shadow charts, independent databases, or "orphan systems," as they are sometimes called, are among the most controversial and difficult to manage forms of protected health information (PHI) that exist. Yet some providers are having success using HIPAA's privacy and security standards to enhance safeguards for this information.

Shadow charts are typically paper copies of original records retained apart from the primary custodial area. Independent databases of clinical information are often created by researchers and may or may not include the same content as the primary health record. While these two types of records are sometimes lumped together, they cause different problems and may require different solutions for safeguarding them.

EHR Eliminates Shadow Charts

Organizations create shadow charts for various reasons. In some cases, physicians in disparate care locations have found that primary records are not always accessible and as a result created copies for subsequent reference. In other cases, physicians create them for use in their professional billing. Unfortunately, these copies may not be as current as the primary record because of others' contributions to the primary record, or they may inadvertently contain originals that never get to the primary record, which causes the primary record to be incomplete.

In addition, information released from shadow charts may never get documented, so there may not be appropriate patient authorization or tracking of disclosures for accounting. These records often do not have formal record processing procedures or safeguards. For example, the records may be stored in open shelves in publicly accessible areas or file cabinets in public corridors. And if they are not linked via an enterprise-wide master person index, the efficiencies of HIPAA's one-time notice of privacy practices and the benefits of common policies and procedures may be lost.

Some organizations that have struggled with providing a unit record to all locations when needed have officially sanctioned satellite record areas, hoping still to achieve only one complete record of care at least within a certain specialty or location. In an officially sanctioned satellite record area, more formal record processing can be applied and because the record's existence is known, it can be pulled together to create a unit record when needed.

Obviously, an electronic health record (EHR) system in which information is available to anyone at any time would be ideal. Many factors are converging to heighten interest in EHRs, such as the recent focus on patient safety. Similarly, HIPAA's goals and standards for privacy and security are drawing significant attention to the EHR. At the same time, satellite locations are finding they don't want the responsibility associated with managing disclosures.

Maintaining multiple record systems that are more or less automated is costly and prone to security problems, especially as each may be differently configured. EHR systems do not happen overnight, so in the meantime, more centralization of functions with respect to release of information is occurring. Over time, shadow charts may disappear.

Independent Databases Contain PHI

Databases that have been independently created (generally by physicians for research purposes) are subject to the same issues as shadow charts: No one really knows which record is most complete, plus there may be ownership and compliance questions as well. While independent databases tend to be a more common problem in academic medical centers than other locations, there may well be such databases in other types of facilities.

Under HIPAA's privacy rule, information may be used for treatment, payment, and operations without special written consent of patients because they have been provided a notice of privacy practices that explains these uses and disclosures. However, use or disclosure for research purposes does require an authorization. Even review of information preparatory to research requires a representation that the information is needed for that purpose and will not be removed from the organization.

Because many physicians view the patients for whom they enter information into their databases as "their" patients, they don't make a distinction between documenting in the primary health record and entering information into a research database. They may also mistakenly believe that the database they are creating is especially secure because no one else has access to it. Or physicians may assume that because they created the database as a researcher (rather than as a covered provider) the content, while clearly individually identifiable health information, is not PHI falling under HIPAA requirements. To that end, they may believe that they own the database and can take it with them when they leave their affiliation with the organization.

Unfortunately, just as with shadow charts, independent databases may contain different information than the primary health record. Because of the burden of documenting in two locations, the independent database may become the primary health record for the physician, especially in a decentralized environment or where controls are lacking over formal record processing. For example, in one organization, lack of security controls on such a database resulted in complete loss of a database that was not only valuable research information but the primary records of care for the patients being seen in that clinic.

Once again, EHRs and HIPAA may provide solutions to independent databases. An EHR can produce a comprehensive unit record and controls can be built in to ensure that information captured is complete with respect to patient care and billing.

Independent research databases that would draw data from such an EHR system could be controlled via application of the security rule's evaluation standard (ß164.308[8]). Formerly named "certification" in the proposed security rule, the evaluation standard would require covered entities to "perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under [the security] rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements."[1] Connectivity of the research database to the primary record system could be contingent upon meeting minimum standards for privacy and security.

HIPAA to the Rescue

There is no mention of shadow charts or independent databases in the HIPAA rules. Because the privacy rule calls for covered entities to define their designated record set, providers may assume that there is only a primary health record system with source data in other systems contributing to the primary record and ancillary systems drawing data from the primary record. The main problem with shadow charts and independent databases is that, over time, they tend to become discrete records. Because they are created under the jurisdiction of the covered entity, they are subject to the covered entity's policies and procedures.

While longitudinal studies and sufficient numbers of cases for research are needed, when records are created for research purposes from a treatment situation, it appears that there is an obligation to obtain institutional review board (IRB) review and patient authorization or IRB waiver for use of any individually identifiable health information.

Because of the complexity of HIPAA's rules, interest in having a central repository of information and management of that information is growing, although this may still be a hard sell to researchers who believe the research databases they create are their personal information. Some academic medical centers have reacted by requesting all patients sign an authorization for release of information to a research database. However, this necessitates a central database should a given patient refuse to authorize such a disclosure.

A central database would also permit control through the security rule evaluation standard to require minimum security measures on all data drawn from the central database. It may not be able to control the disposition of the independent database that is created apart from the central repository.

Security Evaluation Provides Solution

The National Institute of Standards and Technology (NIST) Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Technology Systems," can be used as a guide in developing a Security Evaluation program.[2] NIST defines certification as the "comprehensive evaluation of the technical and nontechnical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements."[3] Accreditation is the "authorization of an IT system to process, store, or transmit information, granted by a management official."[4]

NIST recommends three levels of accreditation:

- Full accreditation means that the system security requirements have been found through a certification process to be satisfied and controls implemented correctly and operating effectively. The system is approved by management to operate in the intended environment and few, if any, restrictions on processing apply
- Interim accreditation means the system does not currently meet the security requirements of the organization, but that mission criticality mandates use of the system. Interim accreditation should be given for a limited and established period of time. Operational restrictions imposed to mitigate the increased risk should be monitored. Resources to complete the action plan and needed certification tasks must be made available
- Accreditation disapproval means the system does not meet the security requirements and controls, residual risk is too great, and mission criticality does not mandate immediate operational need, therefore approval to operate or continue operation is denied. Accreditation disapproval implies that the system probably needs replacement, but resources to do so are either not currently available or left to the department or individual to acquire. In the case of independent research databases, accreditation disapproval may mean that the researcher would have to seek funding for system replacement outside of the covered entity

Implementing a security evaluation program for independent databases can be a challenge if there are many such databases. It is not uncommon for academic medical centers to have 50, 100, or even 200 or 300 such databases. Most data centers are not equipped to handle either the evaluation process or the remediation activities necessitated by the process. As a result, some organizations have chosen to adopt an automated security evaluation program on an honor system, subject to audit. They are conducting this process over the period of time given to implement the security rule in anticipation of the need for considerable time to remediate most systems.

One organization is considering adopting an automated system whereby all independent database custodians must log on to a secure intranet site and respond to questions about their privacy and security policies and procedures, other administrative and physical safeguards, and technical controls. Responses would be scored automatically and the level of accreditation provided, followed by a report sent to senior management.

For this institution, the incentive is continued billing resources for physicians in the faculty practice plan with at least an interim accreditation. However, the organization is awaiting approval to discontinue access to the central billing system if accreditation is disapproved or remediation is not timely. They anticipate an increase in data center workload, although they have also indicated that many researchers will have to seek external funding for improvements where the systems were purchased initially with grant funds.

Other Organizations Have Learned These Lessons

Unfortunately, academic medical centers and research data seem to be most vulnerable to security incidents. Of all the recent news reports of security incidents in healthcare, the majority have occurred in university settings. For example, the University of Washington's security incident is an excellent case study of lessons learned.[5] HIPAA is finally an opportunity to rein in the problems associated with shadow charts and independent databases.

Notes

1. *Federal Register*, Vol. 68, No. 34, Page 8378.
2. Ross, Ron, and Marianne Swanson. "Guide for the Security Certification and Accreditation of Federal Information Systems; NIST Special Publication 800-37, Second Public Draft." National Institute of Standards and Technology, June 2003. Available at http://csrc.nist.gov/sec-cert.
3. *Ibid.*, p. 54.

4. *Ibid.*, p. 53.
5. Dougherty, Michelle. "Handling a Security Breach: Lessons Learned." *Journal of AHIMA* 73, no. 2 (2002): 54-55. Available in the FORE Library: HIM Body of Knowledge at www.ahima.org.

Margret Amatayakul *(margretcpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL.*

Article citation:
Amatayakul, Margret. "HIPAA Reins in Shadow Charts, Independent Databases (HIPAA on the Job series)." *Journal of AHIMA* 74, no.9 (October 2003): 16A-C.