

3/31/03

**Down to the Wire: On the Brink of HIPAA**

*By Leslie Ann Fox, MA, RHIA, and Gwen Hughes, RHIA*

*Thank you to Advance Magazine for permission to use this article*

As we approach the dawn of the “age of the HIPAA” privacy rule on April 14, preparations for compliance are at fever pitch. Every health information management (HIM) director that I visit tells me that HIPAA compliance is at the top of her “to do” list. While my colleague Patty Thierry is on vacation this month I have called upon another colleague, Gwen Hughes, RHIA, business development consultant at Care Communications Inc. and former HIM practice consultant for the American Health Information Management Association, to bring us up to date on the state of HIPAA preparedness.

**Leslie:** Do you think everyone has completed the preparations necessary to comply with the HIPAA privacy rule on April 14, 2003?

**Gwen:** Unfortunately, I do not. I think most organizations will have their notice and authorization forms in place by April 14. However, there are other processes that are not yet completely in place.

**Leslie:** What parts of the privacy rule have been particularly challenging to HIM professionals?

**Gwen:** One area that stands out is the accounting of disclosures standard. This standard requires that covered entities provide individuals who request it with an accounting of disclosures that were made without written authorization from the individual.

**Leslie:** As I understand it, this accounting, as defined in the privacy rule, must include some disclosures that may not have been tracked in the past.

**Gwen:** That’s right. For example, the emergency department must document disclosure of gunshot wound information to local law enforcement, unless the emergency department first obtained the individual’s permission to make such a release.

**Leslie:** What about disclosures made to researchers?

**Gwen:** They must also be tracked, unless the individual provided a written authorization for disclosure of the information. Tracking may take the form of a notation in the accounting of disclosure log, or for research on 50 or more individuals, a description of the research protocol and how the individual can contact the researcher.

**Leslie:** It sounds like one challenge will be to implement systems to track disclosures made by all departments in the health care organization.

**Gwen:** Making sure all departments are included in a central tracking system is very much on the minds of

HIM professionals. Additionally, implementation of the accounting of disclosure requirement is challenging for several reasons:

- There are several exceptions to the tracking requirement and it may be difficult for employees to consistently remember what they do and don't have to track;
- State law may require the tracking of a particular disclosure even though the privacy rule does not require that the disclosure be tracked;
- Many organizations don't yet have an automated tracking system that will combine disclosures made from various departments throughout the organization;
- When tracking must be done manually, it is difficult to combine the information contained in disparate tracking systems throughout the organization.

**Leslie:** As if that's not enough, do any other areas stand out as particularly challenging?

**Gwen:** The other standard that comes to mind is the minimum necessary standard. Although those of us in health care have traditionally limited the information we request or disclose to that which the requester "needs to know," the minimum necessary standard takes that principle further.

**Leslie:** How does it do that?

**Gwen:** The minimum necessary standard requires policies and procedures to limit the information requested or disclosed for routine requests and disclosures. In addition, it requires the development of criteria for limiting the health information requested or disclosed for non-routine requests and disclosures.

Covered entities are also required to identify the people or classes of people in their workforce who need access to protected health information to do their jobs. Then, for each individual or class, the standard requires that covered entities identify the category or categories of protected health information to which they need access to carry out their duties. Finally, the standard requires that covered entities make reasonable efforts to limit access to the minimum necessary to carry out their jobs.

For example, the HIPAA privacy rule implementation team must determine whether everyone who gets the surgery schedule needs the schedule and all the information contained on it. It may mean reducing the amount of information placed on the schedule or hiding some of the information from users who don't need everything provided.

**Leslie:** In working with health care organizations on preparation, what are the priorities as the implementation date approaches?

**Gwen:** I suggest the following:

1. Attend first to individual rights. If your organization has yet to achieve full compliance with the privacy rule, attend first to those privacy standards that address the rights of the individual. According to the privacy rule, the individual has a right to: Inspect and obtain a copy of his or her health information; amend protected health information; an accounting of disclosures; request restrictions on certain uses and disclosures of his or her protected health information; and confidential communications.
2. Avoid reinventing the wheel. Before your organization begins developing its own tools, check AHIMA's HIPAA Community of Practice or search the Web for samples.
3. Implement an electronic accounting of disclosure system wherein disclosures by all departments are recorded in one electronic database. Make sure the software supports the efficient recording of one type of disclosure to multiple individuals (for tracking disclosures to researchers, or multiple disclosures to the

government).

**Leslie:** Have you started to see some innovative best practices emerge?

**Gwen:** These are some of the practices that people are starting to implement that certainly are sensible. I would urge your readers to consider the following:

1. Document the rationale for decisions. From time to time, it will be necessary to decide whether a practice is reasonable for your organization. Document the decisions made and the standards and rationale on which those decisions are based. Such documentation may prove helpful in avoiding a fine should an organization's practices be challenged by the Office of Civil Rights.
2. Circulate educational materials. It will be a challenge to keep privacy "top of the mind." A 15-minute in-service to members of the workforce once a year will prove insufficient. Organizations will find it helpful to share and circulate privacy programs. One organization might purchase and show its workforce a videotape on privacy one quarter, while another develops a Jeopardy privacy game. These organizations can then trade activities the following quarter.
3. Test compliance. Measure compliance with the rule as part of the organization's compliance or performance improvement program.
4. Establish a privacy team whose duties include continuously evaluating uses and disclosures of protected health information to make sure practices remain reasonable for the organization. For example, the fact that almost everyone in the patient accounts department in one hospital can access every patient's electronic health record (EHR) may be reasonable today, given the duties of those individuals and the limited capabilities of that organization's computer system. Such access may be unreasonable, however, after installation of a software upgrade that provides for role-based access.
5. Put your authorization form on your organization's Web site. Enable requestors to either fill it out and submit it online or to print it, complete it and fax it to your organization. This will make it easier for the release of information staff to make sure that the authorization has all of the required information.

**Leslie:** Thank you, Gwen, for so many helpful hints. As the health care industry continues migrating to EHR and eHIM practices, the public can be assured that our professions' commitment to patient privacy is as strong as ever. They can be confident that the most stringent procedures for protection of personal health information are being implemented.

*Leslie Ann Fox is president and CEO, and Gwen Hughes is a business development consultant for Care Communications Inc., a HIM consulting and staffing firm in Chicago. They invite readers to send their thoughts and opinions on this column to [lfox@care-communications.com](mailto:lfox@care-communications.com) and [ghughes@care-communications.com](mailto:ghughes@care-communications.com).*