Tackling ARRA's Privacy Provisions: How One Organization Is Addressing the New Requirements

By LaVonne R. Wieland, RHIA, CHP

Although many have focused on its health IT provisions, the American Recovery and Reinvestment Act (ARRA) also includes significant privacy provisions. HIM professionals should read through the various provisions and outline how each is going to affect their organization and what they need to do to prepare and comply with the provisions.

HealthEast Care System in Saint Paul, MN, began tackling ARRA's privacy provisions by raising awareness, leveraging its HIPAA compliance task force, determining the planning that can begin now, and identifying the questions that still need answering.

Making a List

HealthEast consists of three acute care hospitals, a long-term acute care hospital, multiple physician clinics, medical transportation, home care, and other services, with more than 7,000 employees. In 2001 the organization created a HIPAA compliance task force to oversee the implementation of the HIPAA privacy and security compliance programs and to approve related policies and procedures.

The task force reports to the compliance committee, and although the members and frequency of meetings have changed over time, the group still exists today. This is where the organization began its education process on the new privacy provisions. The group's next meeting was scheduled for late March, approximately a month after the act was signed, so HealthEast's information privacy director had time to prepare the new to-do list of privacy topics.

The director's approach was two-fold: identify the big topics and determine the timelines. Three changes were effective immediately:

- Enhanced enforcements by way of tiered penalties
- The right of state attorneys general to bring civil lawsuits on behalf of residents in their respective states
- Periodic audits by the Department of Health and Human Services (HHS) to assess compliance relative to privacy and security

There was nothing that could be done to prepare for these changes other than to notify staff.

Security Breach Notifications

HealthEast's number-one priority was addressing the security breach notification changes. ARRA required HHS to issue interim final regulations in August 2009, with an effective date 30 days later. The interim final rule defines encryption or destruction as the technology or methodology that will deem information to be secured.

Even before the final regulations were available, a number of issues had to be addressed, including:

- Determining which actions fit the ARRA definition of a security breach
- Deciding how to train staff on what is or is not a security breach
- Establishing a process for staff to report breaches so they could be tracked and reported to the federal government and to the individuals whose information was breached

Immediately a group was convened to begin addressing these questions. The group included the information privacy director, compliance officer, chief information officer, information security director, and system director of health information services.

Many staff naturally sought black-and-white examples of a breach. The group decided obvious security breaches included a fax misdirected to an external party, copies of records sent to the wrong recipient or location, or employee access of a patient record without a work-related reason.

Other situations were more difficult to determine. ARRA provides an exception for an inadvertent disclosure to an unauthorized person who would not reasonably be able to retain the disclosed information.

Staff can retain information in different ways (e.g., photographic memory). So how does an organization know if staff are retaining information that they read or overheard and never knowingly passed on to someone else? How does an organization ensure that the correct instances are reported? And how does an organization ensure that all staff are aware of this information at all times?

HealthEast decided to continue with its current practice of categorizing potential privacy or security breaches by type, such as inappropriate disclosure, inappropriate access, or theft.

Because the organization's current notification requirements did not include notification of individuals when a breach occurred, HealthEast had to modify some of its processes. It worked with its human resources departments to ensure that the privacy office was informed of all breach investigations in a timely manner.

This communication would be critical to meet ARRA's requirement that individuals be notified of the breach no later than 60 days after its discovery. The privacy office would determine what needed to be reported either annually or immediately to HHS or the local media. The privacy office then would initiate any patient notification letters.

HealthEast will also need to ensure its business associates notify the organization of any security breaches that occurred in their handling of patient information. Since business associates will need to comply with the HIPAA security regulations this should not be an issue. However, the compliance dates do not coincide. Organizations must comply with the security breach notification now, while compliance with security regulations is not required until February 2010.

Additional Topics to Be Addressed

Other topics will need to be addressed prior to February 17, 2010. Some will have further guidelines issued by HHS in the coming months. Until the organization knows what those guidelines are, it is difficult to fully prepare for any changes.

Some of the topics still to be addressed, and related questions to answer, include:

Business associates agreements. Business associates will have to comply with the HIPAA security regulations as of February 17, 2010. Business associate agreements may need to be revised to incorporate these changes. Now that business associates are covered entities, whose agreement will be signed—the hospital's or the business associate's? Or will healthcare organizations and business associates sign each other's agreements?

Request for restrictions. ARRA gives patients the right to restrict their protected health information from disclosure to a health plan if they pay for the service in full at the time of service. How can organizations "hide" that information from a health plan? Does it need to be entered as a separate encounter set up as a self-pay, even if other services were provided and billed to the health plan?

Disclosures limited to the limited data set or minimum necessary. ARRA states that minimum necessary will be determined by the person disclosing the information rather than the person requesting the information. Further guidance on the definition of minimum necessary is expected in the coming months.

Accounting of disclosures. Patients can request an accounting of all disclosures for the past three years if their protected health information is maintained in an electronic health record. This is a change from the current process, as disclosures related to treatment, payment, and healthcare operations were excluded. The effective date varies depending on when the organization implemented an electronic health record. The earliest date is January 1, 2011, for entities that purchase systems after January 1, 2009.

Access to PHI electronically. ARRA gives patients the right to receive their information electronically and restricts organizations from charging a fee for the labor only. What use will the information be if the organization has encrypted the information to ensure its security? Will an organization be able to accept information from a patient in electronic form? How does an organization ensure there are no viruses or that it can read it—especially if it is encrypted?

Given ARRA's varied effective dates, this elephant can be eaten in small quantities. However, organizations must begin their planning early.

ARRA Updates

For news, analysis, and resources visit http://journal.ahima.org and www.ahima.org/arra [web page no longer available].

LaVonne R. Wieland (lwieland@healtheast.org) is the information privacy director at HealthEast Care System in Saint Paul, MN.

Article citation:
Wieland, LaVonne R.. "Tackling ARRA's Privacy Provisions: How One Organization Is Addressing the New Requirements" *Journal of AHIMA* 80, no.10 (October 2009): 52-53;58.