Integrating ARRA: Leveraging Current Compliance Efforts to Meet the New Privacy Provisions

By Sandra Nunn, MA, RHIA, CHP

Within the American Recovery and Reinvestment Act, the section known as the HITECH Act provides a combination of incentives and penalties to reduce healthcare costs by automating healthcare records and streamlining health IT. It also broadens the definition of what healthcare information must be safeguarded. These new privacy and security requirements significantly expand HIM's organizational influence.

HIM managers have little time to lose to comply with these provisions, as HITECH provided only one year to prepare for the enforcement of most sections. The new breach notification measures, discussed below, are in effect now and require full compliance by February.

Differentiating the new HITECH provisions from the existing HIPAA rules is only one part of a successful compliance plan. Leveraging existing efforts to comply with e-discovery requirements, state regulations, and other legal or regulatory expectations will take HIM professionals part way down the road to HITECH mastery, provided HIM principles around regulatory compliance have been followed all along.

Access to and Release of PHI

The 2006 amendment to the Federal Rules of Civil Procedure (FRCP) has already alerted healthcare organizations with partially or fully implemented EHR systems that soon they will not be photocopying paper charts for release of information. The FRCP grants the right of electronic access to systems containing protected health information (PHI) if that form of release of information is requested for legal proceedings.

Acknowledging the growing likelihood that PHI will be accessed or released electronically, HITECH calls for an accounting for disclosures of PHI for all disclosures from an EHR. While HITECH expands the disclosure accounting requirements to include treatment, payment, and operations, it reduces the time period that must be documented and limits it to what is released from an EHR. Accounting of disclosures under HITECH must be provided for three years prior to request, rather than the required six years for HIPAA-covered disclosures.

Administering this accounting for disclosures in coordination with existing HIPAA regulations and state laws will require sophisticated HIM release of information staff or the provision of vendor access to a number of a covered entity's clinical systems, thereby increasing the risk of PHI breaches. Careful attention to the HIM infrastructure will help those committed to continuous risk mitigation.

HITECH addresses access rights in the context of the EHR. A covered entity is required to provide copies of PHI electronically to the individual or, at the individual's request, to send the information to a designated person or entity electronically. Thinking back to the FRCP, transmission of this kind exposes the metadata associated with the record to the receiver. Therefore, HIM staff need to understand that this electronic release exposes more information than sending hard copies.

Information services should engage HIM professionals in the task of electronic disclosure accounting, which may take place from multiple systems.

Although many organizations try to control routine release of information through their HIM staff, it is inevitable that clinicians will release information they deem necessary for continuing care. This is where HIM will need to work closely with IS and clinical staff to determine how these disclosures can be gathered centrally for management over the three required years.

HIM managers will also need to work with clinical staff to discourage the practice of releasing PHI after the patient has been transferred or discharged unless for continuity of care. In the paper world, the chart arrives in HIM after discharge or transfer. The electronic record, however, may be left open for completion for some days after the encounter, leaving the door open for disclosure. It is good faith practice to release patient information in as complete and final a state as possible, and clinician release of information after patient departure must be discouraged.

The fees associated with costs to copy paper records usually accounted for paper, toner, and employee time to retrieve records. HITECH allows covered entities to impose fees for access to EHRs and their content, but the fees must be limited to the actual labor costs. With multiple clinical systems contributing content to EHR content, assessments of costs to allow access to several systems or to release information from those systems will require different cost measurements from those associated with a paper-based world.

Determining the routine cost of releasing electronically stored information will ease the determination of cost assessment if an organization finds itself in an e-discovery lawsuit.

Breach Notification

Some states have enacted requirements that organizations notify patients if their PHI has been breached. Under ARRA, breach notification becomes every healthcare organization's responsibility, the rules varying only by the number of patients involved and the means of notification.

ARRA requires notification to patients "without unreasonable delay," but no later than 60 days after the discovery of the breach. In addition, if more than 500 patients are involved, immediate notice to the Department of Health and Human Services (HHS) is required as is public notice in "prominent media outlets."

ARRA defines a breach as the unauthorized acquisition, access, use, or disclosure of PHI. This disclosure must compromise the privacy or security of the information (i.e., the information is not encrypted in any manner). HHS provides guidance concerning what it considers "unsecured PHI," and it will update this information over time.

There is some flexibility with breach notification; unintentional access by an employee or other person acting under authority of a covered entity or business associate is forgivable provided the PHI was reviewed in good faith, under the employment umbrella, and was not further accessed.

Implications of the breach notification regulations may seem only remotely related to HIM operations but in reality can have serious weight for the department. HITECH covers breaches of PHI that occur from any media, including paper.

HIM managers have traditionally kept tight controls on hard-copy records as they moved around their organizations and eventually into storage. However, in an EHR world that is still partially hybrid, it is useful to review how records travel through the healthcare system and how they are sent to storage.

In the electronic mode, security staff are now busy analyzing risk assessments for weak spots where breaches could occur. HIM can prospectively review workflows, particularly those concerning release of information, in their own domains and determine any gaps that may need to be addressed.

HITECH allows state attorneys general to bring civil actions in federal court on behalf of state residents when the attorney general has reason to believe that an interest of one or more residents has been threatened. Thus a review of state breach provisions is in order. Many of these state guidelines are for breaches of financial information and may not apply to PHI leaks.

HIM professionals would be wise to join with IT staff to determine how electronic clinical records are archived and what actions are taken to eventually destroy them. Like the good faith practices that are the foundation of a defense in an e-discovery lawsuit, consistently followed policies and procedures for the retention and destruction of paper, film, or other hard-copy records, including the disks and tapes employed by IS storage staff, must be followed so that PHI cannot be reconstructed.

This is not remarkably different than current practices. However, HITECH requires that electronic media must be cleared, purged, or destroyed according to guidelines in the National Institute of Standards and Technology publication "Guidelines for

Media Sanitization."

Sandra Nunn (snunn@phs.org) is enterprise records manager at Presbyterian Healthcare Services in Albuquerque, NM.

Article citation:
Nunn, Sandra L.. "Integrating ARRA: Leveraging Current Compliance Efforts to Meet the New Privacy Provisions" *Journal of AHIMA* 80, no.10 (October 2009): 50-51.