Reassessing Privacy and Security Compliance: ARRA Provisions Require Organizations Re-examine Procedures and Training

By Dan Rode, MBA, CHPS, FHFMA

Recent federal laws and regulations require healthcare entities abide by new privacy, confidentiality, and security rules. This will require entities to dust off old regulations, review processes and programs, and train and retrain employees and HIPAA business associates.

Training and Retraining Needed

The addition of new federal privacy and security provisions does not relieve covered entities of their ongoing HIPAA training requirements. Entities must continue to provide HIPAA training to "employees, volunteers, trainees, and other persons whose conduct in the performance of work for a covered entity is under the direct control of such entity, whether or not they are paid by the covered entity."

In addition, they must train all workforce members who could possibly be involved with protected health information (PHI). This includes current and new employees, as well as retraining staff when changes occur in an organization's rules, policies, or procedures.

The American Recovery and Reinvestment Act (ARRA) extends some HIPAA privacy and security provisions and adds new regulations that affect all workforce members.

ARRA establishes the first federal regulations on breach notification, setting strict notification timetables and documentation requirements. Organizations must ensure their workforce is aware of these rules, how they are to be applied, and the procedures and policies for complying with them.

HITECH extends some HIPAA requirements to business associates. BAs may not be fully aware of their new responsibilities or may not have begun training. Covered entities should consider assisting their BAs with training as needed.

In addition, the Federal Trade Commission's Red Flags Rule goes into effect November 1. The rule will require that organizations train their staffs on "red flags" that signal possible identity theft. The fact that the data stolen in such a situation might also qualify as protected health information suggests that organizations can and should combine their HIPAA, ARRA, and Red Flags training.

Revisiting BAAgreements

The breach notification requirements provide an immediate need for organizations to reexamine and revise their business associate agreements.

The requirements do not address how a BA and a covered entity will work together when a breach notification is necessary; however, this will become a key element in their relationship. In addition, the rules establish related guidance on methods to secure PHI. Partners must discuss and determine how they will handle data and security requirements for PHI held between them and with any other agents that might be involved.

In addition, HITECH provides that health information exchange organizations become BAs to HIPAA entities involved in the exchange, adding another relationship to the mix for HIPAA entities and requiring new BA agreements.

One caution: while not all HITECH final requirements have been written or have gone into effect, organizations should review the privacy section (subpart D) before considering a revision or new business associate agreement.

HIPAA entities, especially hospitals and large clinics, have a variety of partnerships. They should become familiar with the Federal Trade Commission breach notification requirements if engaged with vendors of personal health records and related entities identified in the rule.

Ensuring Data Security

As HHS and the Office of the National Coordinator for Health Information Technology have rolled out the various ARRA and HITECH rules, they have repeatedly stressed the need for data security, especially when talking about electronic health records (EHRs) and health information exchange.

In August the HHS secretary moved the oversight for HIPAA security from the Centers for Medicare and Medicaid Services' Office of Electronic Standards and Security to the Office for Civil Rights, which has been overseeing HIPAA privacy compliance.

The HIPAA security rule was written to apply to organizations of different sizes and situations. But it also calls for security measures to be "reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information" as described in the rules policies, procedures, and documentation requirements section.

Covered entities must pay strict attention to the requirements spelled out in the HIPAA security rule with the increased attention to auditing compliance, the current rules being altered and new rules initiated, and the potential for investigations into issues such as breaches.

The adoption of EHR systems being encouraged under ARRA also means that the systems environment is changing and systems compliance reviews and necessary training are required on an ongoing basis. Security will be a part of the ARRA "meaningful use" requirements coming later this year, as will security criteria applied in the certification of EHRs. All of these aspects must now enter a covered entity's practices, policies, and compliance activities.

HIM Skills Required

ARRA also calls for a healthcare workforce to facilitate and manage the adoption, implementation, and use of EHRs and electronic health information exchange. The requirements above are just a part of the knowledge necessary to undertake these tasks. Outside of those currently involved or being educated in HIM, few have the credentials for this workforce.

HHS and the Office of the National Coordinator announced a number of health IT technical assistance and education programs in August. It is crucial that the HIM profession ensure that these programs include the HIM curriculum needed for individuals that will undertake the adoption and implementation of EHRs. This is a task that must be done at the local level as well as nationally.

Workflow, release of information, privacy, and security are but a few of the elements that must be understood to help providers adopt and use EHRs effectively and efficiently. States, regional centers, and other entities that are engaged in this unique effort should share their expertise to ensure others receive the training, education, and guidance that will make this effort a successful one.

Dan Rode (dan.rode@ahima.org) is AHIMA's vice president of policy and government relations.

Article citation:
Rode, Dan. "Reassessing Privacy and Security Compliance: ARRA Provisions Require Organizations Re-examine Procedures and Training" *Journal of AHIMA* 80, no.10 (October 2009): 20-22.