March 2010 Vol. 20 No. 3
The Nation's Leading HIM Resource
advance for Health Information Professionals®

RESOURCE CENTER

By Keith Fulmer and Melissa Dempsey

Ensuring HIPAA Compliance

Under the HITECH Act, many outsourced coders and other vendors could be liable.

IN ADDITION TO funding EHR implementation, the American Recovery and Reinvestment Act of 2009 established separate measures to enhance privacy enforcement and expand the reach of HIPAA data privacy and security requirements. Part of this legislation, the Health Information Technology for Economic and Clinical Health (HITECH) Act, increased the scope of HIPAA with a "flow down" clause that extends its requirements to include the "business associates" of covered entities.

Business associates (BAs) are identified as any vendor that a health care facility allows to access protected health information (PHI), including many HIM professionals working as consultants. Thus, under the HITECH Act, many outsourced coders and other vendors could be liable if the patient data they access is breached and they fail to comply with HIPAA requirements. The HITECH Act also calls for increased enforcement of violations, including monetary penalties for BAs.

Strengthening HIPAA and increasing the enforcement of the security and privacy of PHI are critical steps as the industry moves forward with widespread EHR implementation. Storage and transport of patient data in electronic form can introduce the danger of hackers and other unauthorized users gaining access to patient information.

To ensure the safety of patient data and verify compliance with new HITECH regulations, health care facilities should examine how their vendors are handling PHI. It's imperative that covered entities and BAs revise existing contracts to reflect new obligations and create guidelines for ensuring they are in compliance with HIPAA requirements.

HITECH CHECKPOINTS

When defining a plan of action for proactively protecting PHI in compliance with HITECH requirements, health care facilities should take the following steps:

- *Perform a risk assessment.* Determine who has access to electronic PHI and analyze how they are handling it. Identify the scope, pinpoint threats and data vulnerabilities, and identify controls and security gaps.
- *Assess existing infrastructure.* Ensure that appropriate legal, compliance and security structures exist and meet the stated HITECH requirements.
- *Be prepared to resolve security breaches.* Define policies and procedures, as well as any training and technology needed to mitigate identified risks that could lead to a security breach.
- *Establish an incident response process.* Create a plan for identifying breaches and notifying patients and the Department of Health and Human Services when a breach occurs.
- *Develop HITECH training plans.* Assess staff knowledge of new requirements and implement necessary training programs for HITECH compliance. As the control point for information processing, the HIM department must be especially well prepared for HITECH rules.
- *Keep staff informed.* Communicate all HITECH policies and notify staff of available training and other resources.

For facilities that are concerned about how well their staff members and BAs are able to comply with HITECH requirements, staffing firms can often provide audit services. These firms, which are now defining guidelines to ensure their own staff members are compliant when providing services to health care facilities, can also analyze how well a facility protects its data. Such outside auditors can identify situations in which a facility and its BAs are not in compliance with HITECH requirements and then provide recommendations on how to resolve issues.

Although the HITECH Act's regulations now make BAs liable for the security of PHI, it is ultimately the duty of the health care facility to ensure the security of patient data. Some covered entities may think that because the BA is now on the hook for enforcement and penalties, they need not worry and existing standards can be relaxed. This could not be further from the truth. A patient whose medical record is breached is still the health care facility's customer; it's their reputation on the line, regardless of whether a BA is responsible for the breach. Thus, it is certainly in the best interest of both patients and facilities to ensure that individual health records are always protected and secure. ■

*Keith Fulmer is vice president of Health and Life Sciences and Melissa Dempsey is business process manager for Kforce Inc. (**www.kforce.com**), a professional staffing firm providing contract and direct hire staffing for HIM departments. Consultant services include onsite and/or offsite delivery of coding specialists, APC and DRG audits, coder training programs, HIM directors, transcriptionists, certified tumor registrars, trauma registrars and other outsourced personnel. Contact Fulmer at* **kfulmer@kforce.com** *and Dempsey at* **mdempsey@kforce.com**.