Health care risk

Do HIPAA privacy laws apply to your business?

JULES S. HENSHELL
Of counsel
Semanoff Ormsby Greenberg & Torchia, LLC

(215) 887-3754
jhenshell@sogtlaw.com

Insights Legal Affairs is brought to you by **Semanoff Ormsby Greenberg & Torchia, LLC**

Many business operators know that the federal privacy rules under the Health Insurance Portability Act (HIPAA) apply to health information maintained by "covered entities," such as health care providers and health plans. Fewer know that new regulations, effective September 2013, expand the scope of direct responsibility for compliance.

Now, HIPAA rules directly apply to "business associates" of covered entities.

Business associates, like covered entities, are subject to penalties of $100 to more than $50,000 per HIPAA violation, says Jules S. Henshell, of counsel at Semanoff Ormsby Greenberg & Torchia, LLC. If the violation resulted from willful neglect, the Department of Human Services' Office of Civil Rights (OCR) must impose a penalty of at least $10,000 per violation, which increases to at least $50,000 if the violation isn't corrected within 30 days.

"As recently as December 2013, a dermatology physician practice was required to pay a $150,000 fine arising from the a report of the theft of an unencrypted 'thumb drive' from a vehicle," Henshell says. "That settlement with OCR is a clear signal that covered entities and their business associates are potential targets of HIPAA enforcement actions regardless of their size."

Smart Business spoke with Henshell about managing HIPAA risk in your company.

Who qualifies as a business associate?

A business associate is any entity that creates, receives, maintains or transmits protected health information (PHI) in the course of performing services on behalf of a covered entity. Any business that handles PHI, such as billing and coding companies, information technology contractors, document storage or destruction companies, accountants and lawyers, may be subject to the new regulations. If a business associate uses a subcontractor to perform services that involve handling PHI, the subcontractor must also comply.

Where do companies routinely fail to take adequate action?

Health care providers and their business associates increasingly rely upon technology to record, store and manage data. That data may include PHI.

It is not uncommon for personnel to work remotely or take work home. Employees routinely use personal smartphones or home computers to access business email and documents. Such conduct can promote efficiencies, but it also gives rise to the risk of privacy or security breaches in the absence of adequate technical and physical safeguards.

What preventive actions do you recommend?

Benjamin Franklin got it right when he said, 'An ounce of prevention is worth a pound of cure.' It is not enough to adopt policies and procedures for protecting patient privacy. As in the case of the stolen thumb drive, security breaches may be avoidable if a company establishes, monitors and enforces appropriate safeguards.

Businesses that handle PHI should review and update policies governing patient privacy and evaluate whether they have adequate administrative, technical and physical safeguards to protect the integrity, confidentiality and availability of electronic PHI. They should establish computer access controls, use firewalls, virus protections and encryption; back up data; and implement security policies and procedures to meet HIPAA's expanded scope.

They also need written agreements with business associates and/or subcontractors to protect and secure patient information.

Do you have any other advice?

The new regulations impose significant requirements on business associates to:

- Perform and document a risk assessment of computer systems and portable devices.
- Implement administrative, technical and physical safeguards to protect the integrity, confidentiality and availability of PHI.
- Enter into and perform in accord with a written business associate agreement with covered entities to protect privacy and security of PHI.
- Report privacy breaches and security incidents to the covered entity.

Health care providers routinely require contractors to sign business associate agreements containing indemnification provisions that increase responsibilities and risks. Before signing, determine whether your business really is a business associate. ●