

## Are your business associates accountable for HIPAA compliance?

Posted By [Dom Nicastro](#) On February 18, 2011 @ 9:46 am In [Business Associates](#), [HIPAA Violations](#) | [No Comments](#)

HITECH intends to beef up HIPAA compliance among business associates (BA) that handle PHI.

It calls for covered entities to update their BA contracts to reflect the changes outlined in the legislation.

Further, proposed HITECH regulations make BAs directly liable for HIPAA breaches, and subcontractors of BAs must also comply with HITECH and HIPAA. And that means they must comply with the HIPAA Security Rule and the use and disclosures provisions of the HIPAA Privacy Rule.

But is HITECH alone enough to ensure BAs and their subcontractors comply?

Not really, says **Rebecca Herold, CISSP, CIPP, CISM, CISA, FLMI**, of Rebecca Herold & Associates, LLC, of Des Moines, IA.

A contract satisfies HITECH requirements. In it, make sure you include language that requires physical safeguards and asking BAs to document and prove their security measures and plans for incident response.

Case in point – a [breach in Manhattan](#) <sup>[1]</sup> affects 1.7 million patients. It is the largest breach since OCR [began posting breaches on its website](#) <sup>[2]</sup> in February 2010.

On February 9, The New York City Health and Hospitals Corporation (HHC) [reported on its website](#) <sup>[3]</sup> that it began to notify 1.7 million patients, staff, contractors, vendors, and others who were treated by and/or provided services during the past 20 years.

HHC said the breach involves a reported theft of electronic record files that contained PHI, personal information and personally identifiable employee medical information (PIEMI).

The loss of this data, HHC said, occurred through the negligence of a “contracted firm that specializes in the secure transport and storage of sensitive data.”

An HHC spokesman said in an e-mail to **HIPAA Update** the van owned by an information-management company the corporation hired to handle patient records — vendor GRM Information Management Services, a contracted firm that specializes in the secure transport and storage of sensitive data.

In other words, a BA of HHC.

As a result of this theft, HHC said it took additional actions to further secure the transport of backup data off-site, including:

- Suspending the transport of unencrypted backup files from any HHC facility to off-site storage locations
- Expediting its plan to upgrade critical data to the 256-bit Advanced Encryption Standard, considered by the federal government as the highest level of protection against tampering. At the time of the theft, HHC had already upgraded and encrypted nearly 80 percent of the 1,568 systems applications used throughout the corporation. The upgrade is expected to be completed by the fall of 2011.
- Replacing GRM with a new vendor to handle offsite backup data that will be stored in highly protected facilities that have climate-controlled dedicated tape vaults, secured keycard access, video surveillance and trained personnel

"[This breach] demonstrates why healthcare providers, and all kinds of organizations with sensitive information, need to ensure their business associates to whom they entrust confidential and sensitive information have effective safeguards in place," Herold says. "Counting on just a BA agreement is not enough. Organizations need to go further and require business associates to provide some kind of proof or assurance that they actually have safeguards in place. If they don't obtain some type of assurance, it is likely this type of incident will happen."

Herold says she has audited more than 200 BA information security and privacy programs, and almost all the folks in the information security and IT areas in those organizations had not seen the BA contract.

"[They] had no clue what their acquisitions and contracting department had agreed to in the contracts with regard to information security and privacy activities," she says.

HHC said on its website it "values and protects individuals' privacy and confidentiality and deeply regrets any inconvenience and concern this may create for patients, staff, and others affected... There is no evidence to indicate that the information has been inappropriately accessed or misused."

HHC is providing information and credit monitoring services to all affected individuals who may be worried about possible identity theft.

In breaches like HHC's, use of encryption limits damage, Herold says.

"This incident once more demonstrates why any type of mobile PHI (moving on legs, wheels or otherwise outside of the secured server located within the appropriate facility) needs to be encrypted when in electronic form, and locked securely when in print form."

**Jeff Drummond**, health law partner in the Dallas office of Jackson Walker LLP, agrees, offering the following advice:

"Encrypt. Or at least lock your car doors."

---

Article printed from HIPAA Update: <http://blogs.hcpro.com/hipaa>

URL to article: <http://blogs.hcpro.com/hipaa/2011/02/are-your-business-associates-accountable-for-hipaa-compliance/>

URLs in this post:

[1] breach in Manhattan: <http://www.healthleadersmedia.com/content/TEC-262604/NY-Hospital-Data-Theft-May-Affect-Records-of-17-Million>

[2] began posting breaches on its website:

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>

[3] reported on its website: <http://www.nyc.gov/html/hhc/html/pr/notice-to-patients.shtml>