Health Information Compliance Alert

Case Study: Follow 5 Crucial Steps To Prevent BA Agreement Hazards

Beware of silver-harvesting scams that could put your HIPAA compliance at risk.

If you share your patients' protected health information (PHI) with a business associate (BA) without first executing a signed BA agreement (BAA), that's a mistake that could cost you big.

Watch Out for Silver-Harvesting Scam

Background: On April 20, the **HHS Office for Civil Rights** (OCR) announced a $750,000 settlement agreement with **Raleigh Orthopaedic Clinic, P.A.** for potential HIPAA Privacy Rule violations. OCR alleged that Raleigh Orthopaedic furnished the PHI of approximately 17,300 patients to a potential contractor without first executing a BAA.

As in several other recent HIPAA settlements, OCR launched its investigation into Raleigh Orthopaedic following a breach incident report. The covered entity (CE) reported the breach on April 30, 2013. OCR's investigation revealed that Raleigh Orthopaedic released its patients' x-ray films and related PHI to a potential business partner that promised to transfer the images to electronic media in exchange for harvesting the silver from the x-ray films.

Raleigh Orthopaedic didn't execute a BAA with the company before turning over the x-rays and related PHI. When the company failed to send the electronic media to Raleigh Orthopaedic, the clinic discovered that the company had sold the x-ray films to a recycling company that harvested the silver.

In addition to the $750,000 penalty, Raleigh Orthopaedic entered into a Resolution Agreement and a Corrective Action Plan (CAP) with OCR. Under the agreement and CAP, the clinic must revise its policies and procedures to:

- Establish a process for assessing whether entities are BAs;
- Designate a responsible individual to ensure BAAs are in place prior to disclosing PHI to a BA;
- Create a standard template BAA;
- Establish a standard process for maintaining documentation of BAAs for at least six years beyond the date of termination of a BA relationship; and
- Limit disclosures of PHI to any BA to the minimum necessary to accomplish the purpose for which the BA was hired.

If you want to avoid the same fate, take the following steps:

1. Perform Due Diligence on Your Vendors

So-called "silver-harvesting" scams like the one in the Raleigh Orthopaedic case aren't exactly new. "Several years ago when silver prices were relatively high, there were a number of incidents involving the theft of x-ray films from healthcare providers by thieves who harvested and sold the silver recovered from the x-ray films," attorneys **Elizabeth Hodge** and **Carolyn Metnick** of **Akerman LLP** tell Health Information Compliance Alert.

"In some cases, like the Raleigh Orthopaedic case, the vendor claimed it would digitize the films, harvest the silver, and then appropriately destroy the films and related documents," Hodge and Metnick note. "But in reality, the vendor just harvested the silver from the films, leaving the provider without digital records of the films and no idea where the films

were."

In other cases, scammers posed as film disposal vendors, according to Hodge and Metnick. "The thief then harvested the silver and the healthcare provider had no idea what happened to the x-ray films or, perhaps more importantly, any related paper files such as the paper jacket and associated medical records."

Laurie Cohen, an Albany-based partner attorney with **Nixon Peabody LLP**, has also heard about this type of scam and says "it is a warning that providers are a target and vulnerable. That's why you should perform some due diligence on any company or vendor with whom you're considering doing business.

Protect yourself: "This should include checking **Better Business Bureau** websites as well as requesting a list of references and speaking with such references," Cohen advises. And if you will be releasing or providing access to your patients' PHI, your due diligence should also include "querying the company about its HIPAA privacy and security policies and procedures."

Specifically, to verify a vendor's HIPAA compliance, Hodge and Metnick advise that you ask the vendor the following basic questions:

- Do you comply with the HIPAA Privacy and Security Rules? If so, how?
- Does your organization have HIPAA policies?
- Who is your organization's Privacy and Security Officer?
- Have you and your colleagues been trained on HIPAA compliance?
- What do you do to protect the PHI that you encounter?
- Has your organization conducted a security risk assessment?

2. Focus on Your Risk Assessment

Another important step to take in avoiding the same fate as Raleigh Orthopaedic is to conduct a thorough risk assessment. In your risk assessment/analysis, Cohen advises you ask yourself:

- Where is your PHI?
- Who internally has access to and control over PHI?
- When and how is PHI transmitted within and outside your organization?
- With whom do you share PHI?
- For what purpose do you share or release PHI?

3. Educate Your Workforce

Your employees need to understand the internal process to assess the purpose for the release or disclosure of PHI, whether it requires a patient authorization or may be released to a third party who is acting as a BA, Cohen states. Make sure your employees understand what or who is a BA. Instruct all employees that, prior to releasing PHI to a BA, they must confirm that there is a signed BAA in place.

Also train your workforce members on incident reporting, Hodge and Metnick advise. And involve staff in conducting security audits and assessments.

4. Provide Access to Only the Minimum Necessary

To the extent that you provide a BA with access to PHI, you need to assess how much PHI the BA needs to perform its activity, Cohen says. You should always limit the access to the minimum necessary.

Example: "If a vendor is shipping medical supplies to a patient's home on behalf of a home care agency that will be using such supplies as part of its services, the vendor will likely need no more than a supply list and the patient name and address for shipping," Cohen illustrates. "The vendor will not likely need the patient diagnosis or other health information to fulfill the order."

5. Get a Firm Grip on Your BAAs

Cohen stresses that you should develop a template BAA. You should also designate one or more individuals who will have the authority to negotiate and execute BAAs. These individuals should be responsible for maintaining:

- A list of all BAs;
- The executed BAAs; and
- A description of the PHI and purpose for which you're releasing it to the BA.

Important: Keep in mind that if OCR selects you for a HIPAA audit, one of the first things you'll need to produce is a list of all your BAs and the corresponding BAAs.

You should also create a process for assessing current and future business relationships to determine whether they constitute BA arrangements, Hodge and Metnick advise. And in your BAAs and/or service agreements, you should consider defining:

- How and for what purpose the BA will use or disclose PHI;
- How a vendor will report to you any use or disclosure of PHI not provided for by the BAA or contract, including breaches of unsecured PHI and security incidents;
- The timeframe for when the BA should report any breach, security incident or cyber-attack to you; and
- The type of information the BA should report to you when alerting you to a breach or security incident (such as a description of what happened, date of the incident, date of discovery, type of PHI involved, and a description of what the BA is doing to investigate the incident and protect against future incidents).

Resources: To read the Resolution Agreement and CAP, go to www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/raleigh-orthopaedic-clinic/index.html. Model BAA language from HHS is available at www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.