Write, revisit BAA policies that protect you when associates mess up HIPAA

by: Roy Edroso

Published Jul 11, 2016

Last Reviewed Jul 7, 2016

HIPAA

A recent Office for Civil Rights (OCR) settlement that fixes responsibility for a HIPAA breach on a business associate underlines the importance of making sure you have proper, current and well-managed business associate agreements (BAAs) for every relevant vendor.

On June 29, OCR came to a $650,000 settlement with Catholic Health Care Services (CHCS) of the Archdiocese of Philadelphia "after the theft of a CHCS mobile device compromised the protected health information (PHI) of hundreds of nursing home residents," per an OCR press release. Notably, in this situation, the nursing homes were covered entities (CEs) under HIPAA and clients of CHCS — and because they had the foresight to engage in proper BAAs with CHCS, the responsibility for this breach fell on the associate, not on the covered entities.

OCR has fined a number of CEs whose PHI was made insecure by vendors, says Rick Hindmand, a member of the McDonalds Hopkins law firm in Chicago, because they didn't have BAAs that would have protected them. Bill Roberts, an associate with Shipman & Goodwin in Hartford, Conn., says this is one of the first major enforcement actions against a business associate in which a CE with a BAA was not found liable.

"With no BAAs, the covered entities would be in violation of the privacy and security rules and potentially subject to penalties," says Hindmand.

Who gets BAAs?

BAAs have been a hot HIPAA topic since the HIPAA mega-rule came out in 2013, codifying the necessity of such agreements (*PBN 9/2/13*). Essentially, you should have one with every vendor who handles your PHI — within reason, say experts.

Jeff Mongelli, CEO of Acentec in Irvine, Calif., concedes that if the vendor's handling of your PHI is "incidental" (that is, not likely to happen in the course of the vendor's ordinary business with you, such as a janitor's occasional handling of a patient chart), a confidentiality agreement would probably be sufficient. Such agreements should "address access to data, security incident reporting and legal responsibilities," adds Roberts. CEs would also have to take reasonable steps to make sure these non-associate vendors don't see too much PHI (*PBN 5/18/15*).

But there are some vendors that do have meaningful PHI access and frequently get overlooked, says Roy Wyman, a partner at Nelson Mullins Riley & Scarborough LLP in Nashville, Tenn. He cites as an example collection agencies that are recovering unpaid treatment fees from patients. Wyman says people get confused because "they know you can reasonably disclose PHI for payment purposes — there's nothing wrong with a doctor calling up a patient to ask for payment. But when you're sending a list of patient names and addresses to a collection agency, you better have a BAA."

Is your BAA good enough?

BAAs have been around long enough that a competent lawyer can probably provide you with a template. But remember, the agreement only protects you from enforcement actions — in case of a breach, you still may want more from the vendor.

"Any time a CE enters into a BAA, you want indemnification or reimbursement language," says Roberts. "For example, you want to be protected from third-party actions. Also, you want to be reimbursed for costs, such as breach notices, hiring a call center, PR, etc. It all adds up."

In fact, if your BAA isn't good enough — or doesn't exist — and there's a breach, you may choose to pursue legal remedies to recover losses from the vendor. "Depending on the state and your circumstances, you may have rights under the vendor services agreement itself regarding violations of the law, loss of data, failure to meet industry standards, negligence, etc.," says Roberts.

3 questions to ask about your BAA policy

Are you keeping track of your BAAs? "A large hospital chain may have thousands of such agreements," says Roberts. "There are many opportunities for miscommunication. Someone may have thought the BAA was signed, for example. Or the contract management software had a check-the-box feature that didn't get checked."

Also, at larger firms "you'll have signature authority with more than one person," says Wyman. "And they don't always get training in proper approval processes before signing documents or understand HIPAA requirements."

You might bring in a HIPAA consultant to establish a protocol that prevents any vendor relationship from going forward until there's been a HIPAA review, says Roberts. Wyman suggests regular BAA audits, done similarly to chart audits. "Establish a benchmark of a certain percentage of BAAs being properly signed — say, 98%, depending on your entity — then pull a certain number of your BAAs and see if they meet the benchmark," he says. Do this for any issues that come up, then write policy and create training to meet the shortfalls.

Has the BAA expired? Roberts advises that BAAs not have expiration dates "and should instead be in effect as long as the third party has access to patient information." Expiration dates can pass without notice, leaving your PHI in the vendor's hands and yourself unprotected. Check whether your current BAAs have expiration dates, move to change that ASAP and, where that's not possible, make sure to get your data out of the vendor's hands.

Do you need to get out of the BAA? Upon reconsideration, you may realize the terms of your current BAA don't comply with HIPAA or fail to adequately protect your organization. Explore your options with legal counsel, but if your vendor is not keen to renegotiate, tell the vendor that negotiating a new BAA is a condition of renewing the vendor's services, says Roberts. If the vendor wants to keep your business, it will cooperate.

If that doesn't work, you may be able to void the contract on the grounds that "it would be illegal for the provider to continue under it," says Roberts. Consider cutting off the vendor's access to your PHI until the matter is resolved. — *Roy Edroso (redroso@decisionhealth.com)*

*(**Editor's note:** Read more about HIPAA and BAAs at the Part B News blog.)*

BACK TO TOP