COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 6. June 08, 2023 Breach Notification Checklist: When BAs Are Responsible, CE Prep Counts

By Jane Anderson

Covered entities (CEs) working with business associates (BAs) and BAs working with subcontractors BAs need to carefully establish who is responsible for specific aspects of breach response before a breach occurs to ensure all goes smoothly in the event of a security incident.

That's the word from three experts on BA agreements (BAAs) and breach response who spoke recently at a national meeting.[1]

"I think it's important just holistically, when you're engaging in these relationships, to think long-term in terms of what obligations go with who," said John Haskell, HIPAA privacy officer at Medline Industries, and a former investigator for the HHS Office for Civil Rights, in offering a checklist for CEs and BAs to follow to make a breach response as effective as possible.

- **Carefully evaluate provisions relating to breach response and attempt to standardize provisions.** Mark Fox, privacy and research compliance officer for the American College of Cardiology Foundation, told conference attendees that the time frame of breach notification is one of the most frequently negotiated items in a BAA, "and that is often complicated by state law as well," which in some cases has a shorter time frame than HIPAA. "So, from our perspective, when we're negotiating, we try to set up our response and our contractual provisions to be consistent with the most stringent timeframe—I believe currently the two states that have the most stringent timeframes are California and Florida."

Thora Johnson, partner and chair of the health care practice at Orrick Herrington & Sutcliffe LLP, in Washington, D.C., agreed that, if possible, organizations should standardize their BAAs' breach notification provisions. However, this obviously may be difficult since "every covered entity wants to have their standard form, and every business associate is going to want to have their standard form," Johnson said. "So, there's often some negotiation as to whose form are you using, depending on relative negotiation strength. But to the extent that you can have a streamlined approach, you'll know that you need to provide notice in X days, say, of a breach, and the simpler your response will be as a business associate."

A BA working as a subcontractor to another BA will be stuck with whatever timeline already exists in the original BAA since "those obligations are passed down," Haskell pointed out. "So, if they say, 'We have a 12-hour timeline notification,' we have to either take it or leave it."

- **Know where your BAAs are located, and keep in mind that the breach response provision is what you rely on for defining roles and responsibilities during a response.** "One of the challenges you have with business associate agreements is significant variation relating to the terms and conditions regarding a breach response. And because many of us maintain thousands of these, it's also making sure that you're readily able to identify where your business associate agreements are and understand that variation," Fox said.