Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

Ensure You Have Business Associate Agreements or Face HIPAA Penalties

Insight — 5/12/2016

The Office for Civil Rights ("OCR") has sent a clear message to covered entities: make sure that you have business associate agreements ("BAAs") or face HIPAA penalties. The OCR recently announced two hefty resolution agreements with covered entities based on their failure to obtain BAAs before disclosing protected health information ("PHI") to their business associates.

The Cases. In March 2016, North Memorial Health Care of Minnesota agreed to pay $1.55 million to settle OCR charges that it violated HIPAA by disclosing PHI to its business associate, Accretive Health, without first executing a BAA. The issue surfaced following the theft of an Accretive employee's unencrypted, password-protected laptop containing PHI of approximately 9,500 individuals. Note that it was the business associate's laptop that was lost, not the covered entity's; nevertheless, the OCR extracted the settlement from the covered entity. The OCR also cited North Memorial's failure to conduct an appropriate risk analysis. For a copy of the press release, click here.

In April 2016, Raleigh Orthopedic Clinic agreed to pay $750,000 to settle OCR allegations that it violated HIPAA by turning over thousands of x-rays and related protected health information to a vendor without a BAA. The vendor had promised to transfer the x-rays to electronic media in exchange for salvaging silver from the x-ray films. For a copy of the press release, click here. In its press release, the OCR reaffirmed,

> HIPAA's obligation on covered entities to obtain business associate agreements is more than a mere check-the-box paperwork exercise. It is critical for entities to know to whom they are handing PHI and to obtain assurances that the information will be protected.

Id. The OCR is obviously serious about BAAs.

The Concerns. The failure to obtain BAAs is clearly a violation of the HIPAA Privacy and Security Rules. Nevertheless, the two cases are troubling for several reasons. First, there is nothing in the published agreements or press releases to suggest that the business associates were acting as the covered entities' agents so as to make the covered entities vicariously liable for the business associate's conduct per 45 CFR 160.400; thus, the covered entities were purportedly punished for their own misconduct, which misconduct appears to be relatively innocuous.

Second, business associates are obligated to comply with the HIPAA

Security Rule and, presumably, mandatory BAA terms, even if no BAA is executed (*see* 78 FR 5574); accordingly, it is difficult to understand how the absence of a written BAA caused or contributed to any resulting damages or warranted such large penalties, especially when the business associate is a sophisticated party such as Accretive Health who surely understood its HIPAA obligations.

Third, it is not clear from the published Raleigh Orthopedic agreement whether the disclosure to the vendor resulted in any further improper use or disclosure to or by third parties. If not, then it is even more difficult to justify a $750,000 penalty because the vendor is obligated to maintain the confidentiality of the PHI regardless of whether a written BAA was executed. If there was no improper loss, access, or disclosure to third parties, where is the harm to justify the $750,000 penalty?

Admittedly, we do not know all the underlying facts that triggered the OCR's response; regardless, the cases serve as a sober warning that the OCR may look to covered entities to pay the price of their business associate's misconduct if there is not an appropriate BAA in place.

Reporting Improper Disclosures to Business Associates. These cases beg another question: under the HIPAA Breach Notification Rule, must a covered entity self-report the improper disclosure of PHI to a business associate if there is no BAA? The disclosure of PHI to a business associate without a BAA is a violation of the HIPAA Privacy Rule, but not all Privacy Rule violations are reportable. A covered entity need not report an improper use, access, or disclosure if there is a low probability that the information has been compromised. *See* 45 CFR 164.402. In its Omnibus Rule commentary, HHS suggested that an improper disclosure to another HIPAA covered entity who is otherwise obligated to maintain the confidentiality of the information may indicate that there is a low probability that the data has been compromised, *e.g.*, where PHI is faxed to the wrong physician's office. *See* 78 FR 5642. If so, then disclosure to a business associate—who is obligated to maintain the confidentiality of the information even if there is no written BAA—would seem to suggest a low probability that the data has been compromised, and hence the disclosure should not be reportable. Nevertheless, covered entities should carefully analyze the facts of each case given the OCR's recent decisions.

Action Items. The recent resolutions should prompt covered entities and business associates to reexamine their relationships and confirm that they have written BAAs in place or face the risk of penalties. If you need help identifying your business associates, we have published a BAA Decision Tree here. If you need help drafting or evaluating compliant business associate agreements, see our checklist.

For questions regarding this update, please contact:
Kim C. Stanger
Holland & Hart, 800 W Main Street, Suite 1750, Boise, ID 83702
email: kcstanger@hollandhart.com, phone: 208-383-3913

only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the author. This news update is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of the law to your activities, you should seek the advice of your legal counsel.
