THE
NATIONAL LAW REVIEW

HIPAA Updates: New Guidance for Business Associates and Continued Data Breaches

Article By
Sarah Beth S. Kuyers
Kate F. Stewart
Mintz
Health Law

- Administrative & Regulatory
- Communications, Media & Internet
- Health Law & Managed Care

- All Federal

Monday, June 10, 2019

The HHS Office for Civil Rights (OCR) released a new guidance document regarding which HIPAA violations business associates (BAs) can and cannot be held directly liable for. In the guidance, OCR states that BAs can be held directly liable for a list of 10 violations but notes that certain other violations, like the reasonable cost requirement for a patient's access to their PHI, cannot be enforced directly by OCR against a BA. The covered entity (CE) is still on the hook for violations of this type, however, so CEs should carefully review their BAAs to ensure that it covers requirements that don't directly apply to BAs but are still enforceable against CEs.

Large data breaches also continue to dominate the press.

- Last week, we discussed on the blog a breach involving an EMR and software

services provider after hackers accessed 3.5 million patient records. You can read more about it here.

- OCR recently announced a settlement in which a diagnostic imaging company, Touchstone Medical Imaging (TMI), agreed to pay $3 million for a breach involving one of its FTP servers that contained PHI for over 300,000 patients. OCR began an investigation after receiving an email alleging that information about TMI's patients, including social security numbers, were publicly available online due to an unsecure FTP server. TMI discovered the breach only after receiving a letter from OCR regarding its investigation. TMI's server had allowed uncontrolled access to certain information, which permitted search engines to index the information and the information to be available online even after the server was shut down. Furthermore, TMI initially stated that no PHI was exposed but subsequently admitted that PHI of over 300,000 patients was involved. The settlement agreement states that OCR's investigation indicated that TMI: failed to enter into a business associate agreement with certain vendors; failed to conduct an "accurate and thorough" security risk assessment; and failed to notify the affected individuals and media of the breach, among other HIPAA violations.

- On Wednesday, LabCorp announced that it received notice from American Medical Collection Agency (AMCA), a collection firm working on its behalf, regarding unauthorized access of 7.7 million patients' PHI stored by AMCA. This announcement followed a similar one from Quest Diagnostics earlier last week, in which Quest reported that AMCA's breach affected 11.9 million of its patients. According to LabCorp's 8-K, the information on AMCA's affected system could include individuals' first and last names, dates of birth, addresses, phone numbers, dates of service, provider names, and balance information.

Also, in case you missed it, our Privacy & Cybersecurity colleagues recently wrote about Nevada's new privacy law, which requires website operators to provide consumers with the right to opt-out of the same of their personal information. We continue to track state law developments, like the California Consumer Privacy Act (see our recent post here), that impact those that operate in the health care industry.