Insights

Protecting Patient Information: The Importance of a Business Associate Agreement Under HIPAA

December 13, 2018

By: Stephanie T. Eckerle and

The Health and Human Services' Office of Civil Rights ("OCR") recently entered into a Resolution Agreement with a Florida physicians' group, Advanced Care Hospitalists PL ("ACH"), after investigating an alleged HIPAA breach.[1] Between November 2011 and June 2012, ACH obtained billing data processing services from an individual who held himself out to be a representative of a third-party billing company (the "Company"). On February 11, 2014, ACH was notified of patient information being accessible on the Company's website. Thereafter, ACH submitted a breach incident report with OCR, which revealed that 9,255 patients were potentially affected by the breach.

Through its investigation, OCR discovered that ACH did not have a business associate agreement with the individual or the Company, thus violating the HIPAA Rules.[2] Although ACH has been in existence since 2005, it failed to implement any risk analysis or security measure policies prior to receiving notice of the 2014 breach.

Under the terms of the Resolution Agreement, ACH was required to pay OCR $500,000 and enter into a two year Corrective Action Plan. The Corrective Action Plan requires ACH to, among other things, provide HHS with an accounting of all of its business associates and maintain business associate agreements; conduct a thorough risk analysis and adopt a risk management plan; and review and revise its written policies and procedures to fully comply with HIPAA Rules that govern covered entities and business associates. Further, ACH will be responsible for distributing HHS approved policies and procedures to all of its workforce members. To see the complete Resolution Agreement and the Corrective Action Plan attached to it, please click here.

OCR's Resolution Agreement with ACH leave covered entities with a few key takeaways:

1. All covered entities must have and abide by HIPAA policies and procedures that, among other things, require the covered entity to enter into a business associate agreement prior to sharing patient information with a business associate.

2. The HIPAA policies and procedures should specify what arrangements are considered business associate arrangements, such as claims processing, data analysis, utilization review, quality assurance, billing, practice management and accounting services.[3]

3. The covered entity should have a procedure in place to ensure that (a) business associate agreements are fully executed and retained by the covered entity; (b) that a list of business associate agreements is kept by the covered entity; and, (c) that audits of the covered entity are undertaken to ensure that all proper business

associate agreements are in place.

4. The covered entity should conduct due diligence on each business associate to ensure that the business associate, as well as its subcontractors, are actually compliant with HIPAA and fulfilling their business associate obligations contained in the business associate agreement. This type of due diligence or audit may include, among other things, asking for a copy of the most recent HIPAA security risk assessment undertaken by the business associate as well as proof of cybersecurity insurance maintained by the business associate.

If you have questions regarding business associate agreements and best practices or other HIPAA-related questions, please contact Stephanie T. Eckerle at seckerle@kdlegal.com, or Alexandria M. Foster at afoster@kdlegal.com, or your regular Krieg DeVault attorney.

1 https://www.hhs.gov/about/news/2018/12/04/florida-contractor-physicians-group-shares-protected-health-information-unknown-vendor-without.html

2 See 45 C.F.R. § 164.502(e), § 164.308(b), and § 164.314(a).

3 45 C.F.R. § 160.103.