THE
NATIONAL LAW REVIEW

$500,000 Settlement for Failure to Comply with Basic HIPAA Compliance Requirements

Drinker Biddle
Article By
Sumaya M. Noush
Drinker Biddle & Reath LLP
DBR on Data

- Health Law & Managed Care
- All Federal
- Florida

Wednesday, December 19, 2018

Advanced Care Hospitalists PL (ACH) and the Office for Civil Rights of the U.S. Department of Health and Human Services (HHS-OCR) entered into a $500,000 no-fault settlement and two year corrective action plan (CAP) to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA).

ACH has provided contracted internal medicine physicians to Florida-based hospitals and nursing homes since 2005. ACH obtained billing data processing services between November 2011 and June 2012 from an individual who purported to be a representative of Doctor's First Choice Billings, Inc. (First Choice), a third party billing company. ACH did not enter into a business associate agreement (BAA) agreement with the third party billing company. The individual who provided these services to ACH allegedly used First Choice's name and website without the billing company's knowledge or permission.

On February 11, 2014, a Florida hospital notified ACH that patient demographic information, including names, dates of birth, and social security numbers, and some limited clinical information was viewable on First Choice's website. First Choice quickly reacted and shut its website down on February 12, 2014. ACH identified 400 affected individuals before it filed its breach notification report with HHS-OCR on April 11, 2014, which it later amended to indicate that another 8,855 individuals could have been affected.

HHS-OCR’s investigation revealed that ACH failed to:

1. Enter into a BAA with the individual who purported to work on behalf of First Choice;
2. Enter into a services agreement with the individual who purported to work on behalf of First Choice;
3. Implement any HIPAA Privacy, Security, or Breach Notification rule policies or procedures until April 1, 2014; and
4. Conduct a risk analysis until March 4, 2014.

ACH’s CAP requires it to undertake a widespread adoption of BAAs, enterprise-wide risk analysis, and produce comprehensive policies and procedures to comply with HIPAA.

As a reminder, HIPAA requires a covered entity to obtain satisfactory assurances from its business associate that it will safeguard whatever protected health information (PHI) and electronic protected health information (ePHI) the business associate creates, receives, maintains, or transmits on behalf of the covered entity. HIPAA also requires covered entities to implement policies and procedures that comply with HIPAA rules as well as conduct accurate and thorough assessments of the potential risks and vulnerabilities to its ePHI. In this situation, OCR determined that ACH did not obtain such assurances from its business associates or implement any appropriate risk analyses and policies and procedures, and as a result violated the HIPAA Privacy and Security Rules.