BuchalterNemer
A Professional Law Corporation

Health Care Client Alert
August 2016

HIPAA Security Rule Compliance for Providers & Business Associates in Three Easy Steps

By: Julie Simer

On August 4, 2016, the Office for Civil Rights ("OCR") of the U.S. Health & Human Services Department ("HHS") announced a $5.55 million HIPAA settlement with Advocate Health Care Network ("Advocate"), the largest fully-integrated health care system in Illinois. According to the OCR, the settlement is the largest to date against a single entity.

The OCR investigation began in 2013 after Advocate reported three separate and distinct security breach incidents. The breaches involved Advocate's subsidiary, Advocate Medical Group ("AMG"), a nonprofit physician-led medical group.

The Advocate settlement is a good example of how a large breach can lead to an OCR investigation. However, health care providers, such as medical groups and hospitals, and their business associates may be unaware that even a small breach may lead to an OCR investigation. Beginning this month, the OCR has begun an initiative to investigate more widely the root causes of breaches affecting fewer than 500 individuals. The OCR has asked its regional offices to increase their efforts to identify and obtain corrective action to address entity and systemic noncompliance related to these breaches.

OCR's recent announcement follows the beginning of phase two of HIPAA compliance audits. On July 11, 2016, the OCR contacted 167 health plans, health care providers and health care clearinghouses for audits, giving each covered entity ten days to respond to the audit request. These audits will primarily be desk audits, although there will be some on-site audits conducted. Business associate audits will begin in the fall. The protocol elements for the audits can be found on the OCR website at: http://www.hhs.gov/sites/default/files/2016HIPAADeskAuditAuditeeGuidance.pdf

On the bright side, the Advocate corrective action plan ("CAP") is useful for evaluating HIPAA Security Rule compliance. The CAP outlines three steps to achieve compliance:

Step One: Assemble the following documentation:

- ✓ Complete inventory of all of the provider's facilities, electronic equipment, data systems, and applications that contain or store ePHI that will then be incorporated into its risk analysis;
- ✓ Comprehensive and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information ("ePHI") held by the provider;
- ✓ Enterprise risk management plan to address and mitigate any security risks and vulnerabilities found in the risk analysis, including a timeline for the provider's implementation, evaluation, and revision of risk remediation activities;
- ✓ Written process to evaluate, on a regular basis, any environmental or operational changes that affect the security of ePHI in the provider's possession or control, including the provider's acquisition of new entities;
- ✓ Written report regarding the provider's encryption status, which shall include:
  - the provider's devices and equipment including, but not limited to, desktop computers, laptop computers, tablets, mobile phone devices, USB drives, and medical equipment, that may be used to access, store, download, or transmit ePHI,
  - the total number of all the provider devices and equipment that may be used to access, store, download, or transmit the provider's ePHI that are encrypted, as well as evidence of such encryption, and
  - an explanation of the total number of unencrypted devices and equipment.

Step Two: Complete a comprehensive review:

- ✓ Review, and to the extent necessary, revise the provider's policies and procedures related to the use of hardware and electronic media including, but not limited to, desktop computers, laptop computers, servers, tablets, mobile phone devices, USB drives, external hard drives, DVDs and CDs that may be used to access, store, download, or transmit the provider's ePHI, and include the following:
  - identify criteria for the use of such hardware and electronic media and procedures for obtaining authorization for the use of personal devices and media that utilize the provider ePHI systems, and
  - address security responsibilities, including disposal and reuse of personal devices and media, and regular compliance monitoring;
- ✓ Review, and to the extent necessary, revise the provider's policies and procedures to limit physical access to all of its electronic information systems and the facilities in which they are housed as follows:
  - ensure that properly authorized access is allowed, and

- include details of physical security safeguards to restrict unauthorized access;

✓ Review, and to the extent necessary, revise the provider's policies and procedures related to business associates and
- designate one or more individual(s) who are responsible for ensuring that the provider enters into a business associate agreement with each of its business associates, prior to the provider disclosing ePHI or non-electronic PHI to the business associate,
- create a process for assessing the provider's current and future business relationships to determine whether each relationship involves a business associate, create a process for negotiating and entering into business associate agreements with business associates prior to the provider disclosing ePHI or non-electronic PHI to the business associates,
- limit disclosures of ePHI and non-electronic PHI to the minimum amount that is reasonably necessary for business associates to perform their duties, and
- create a process for maintaining documentation of business associate agreements for at least six years beyond the date of when the business associate relationship is terminated.

Step Three: Implement an effective training and monitoring program:

✓ Develop an enhanced privacy and security awareness training program, which may be conducted online and/or electronically, using computers and e-learning tools, for all of the provider's workforce members who have access to PHI, including ePHI, and include:
- general instruction on compliance with the provider's policies and procedures related to the HIPAA rules,
- annual training on the provider's policies and procedures related to the HIPAA rules to all active workforce members, as necessary and appropriate for the workforce members to carry out their function,
- training on all of the new and revised policies and procedures to the extent such new policies and procedures are developed and existing policies and procedures are revised,
- delivery of training to workforce members who commence working for the provider, or that are given access to PHI, including ePHI, within thirty days of the commencement of their employment or affiliation with the provider,
- certification, in writing or in electronic form that each workforce member has received the required training and the date training was received,
- retained copies of such certifications for no less than six years following the date training was provided,
- review of the training program as reasonable and appropriate, but no less than every two years and updates to the training program to reflect any material changes in the provider's policies and procedures, federal law, HHS guidance, and/or any material compliance issue(s) discovered during audits or reviews within a reasonable period of time after the material change becomes effective; and

✓ Develop a written description of the provider's plan to monitor internally its compliance with its policies and procedures.

As mentioned above, compliance responsibilities are not limited to health care providers and other "covered entities." The OCR recently settled an enforcement action against a business associate. Catholic Health Care Services of the Archdiocese of Philadelphia ("CHCS") provided management and information technology services as a business associate to six skilled nursing facilities. It agreed to settle potential HIPAA violations after the theft of a mobile device. The total number of individuals affected by the combined breaches was 412, but the settlement required CHCS to pay $650,000 and enter into corrective action plan.

Buchalter Nemer attorneys can help clients develop and implement policies, procedures, and training for HIPAA compliance. By developing a sound compliance program, health care providers and their business associates can avoid unnecessary penalties and possible damage to their reputation resulting from a security breach.

Julie Simer is Special Counsel in the Firm's Health Care Practice Group in the Los Angeles office. She can be reached at 213.891.5117 or jsimer@buchalter.com.