This article is one of a series of articles contracted by SVS to address issues, opportunities and obstacles that have an impact on vascular practices.

Trends in HIPAA Enforcement Against Physician Practices[1]

By: Abby E. Bonjean, Esq., *Polsinelli*

The Office for Civil Rights ("OCR"), the federal agency vested with the authority for enforcing the privacy and security requirements of the Health Insurance Portability and Accountability Act ("HIPAA"), continues to increase its enforcement of the HIPAA Privacy, Security and Breach Notification Rules.[2] Although covered entities, including physicians and physician practices, have been required to comply with the HIPAA Privacy and Security Rules[3] for more than ten years, OCR has been slow to exercise its enforcement authority. However, since the implementation of the Breach Notification Rule in 2009, which requires covered entities to self-report breaches of protected health information ("PHI"), OCR has announced over fifty enforcement actions. In fact, 2016 was a record-breaking year for HIPAA enforcement, with OCR bringing in over $23 million from twelve settlements and one civil monetary penalty. And, although we are just halfway through 2017, OCR has already entered into seven settlements with entities and imposed one civil monetary penalty on an entity for a total of approximately $16 million. Notably, those enforcement activities are not limited to large institutional entities, such as hospitals, but include physician practices.

[1] This Article is for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

[2] Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act, and their implementing regulations, as amended from time to time (collectively, "HIPAA").

[3] The HIPAA Privacy Rule established national standards to protect individuals' health information. The HIPAA Security Rule specifies administrative, technical, and physical safeguards for entities to implement to ensure the confidentiality, integrity, and availability of protected health information in electronic form.

This article summarizes recent enforcement actions against physician practices and discusses some of the recommended best practices to mitigate HIPAA enforcement risks and penalties.

Recent Enforcement Actions

Although many of OCR's enforcement actions involve large health systems, several recent cases have involved physician practices. Specifically, in April, OCR announced potential violations of HIPAA by the Center for Children's Digestive Health ("CCDH"), a six physician gastroenterology practice that operates at seven clinic locations throughout the Chicago area. OCR opened a compliance review of Filefax, a document storage company, after media outlets notified OCR that Filefax, a business associate of CCDH under HIPAA, disposed of hundreds of medical records, including CCDH's records, in a dumpster. By way of context and as a reminder for the reader, business associates are those persons or entities that perform functions on behalf of the covered entity and require access to PHI in order to perform those functions.[4] Included in this category are many types of vendors, particularly EHR vendors, transcription vendors, IT consultants, collection agencies and cloud vendors. OCR's investigation revealed that CCDH began disclosing records to Filefax in 2003 but failed to enter into the HIPAA-mandated written business associate agreement with Filefax until October 2015. CCDH agreed to pay OCR $31,000 and be subject to a two-year corrective action plan to resolve potential violations of HIPAA, including its failure to have an appropriate business associate agreement with Filefax from 2003 through 2015.

In April 2016, OCR entered into a settlement with Raleigh Orthopaedic Clinic, P.A. ("Raleigh Orthopaedic"), a group practice operating clinics and an orthopaedic surgery center in Raleigh, North Carolina. Raleigh Orthopaedic reported to OCR that it had disclosed x-ray films and related health information of approximately 17,000 patients to a potential business partner that promised to transfer the images to electronic media in exchange for harvesting the silver from the x-ray films. OCR found that Raleigh Orthopaedic failed to enter into a business associate agreement with its business associate partner before disclosing the x-rays as required under HIPAA. Consequently, Raleigh Orthopaedic settled with OCR for $750,000.

Additionally, in September 2015, OCR settled an enforcement action with Cancer Care Group, P.C. ("Cancer Care"), a radiation oncology physician practice with thirteen oncologists serving hospitals and clinics throughout Indiana. OCR commenced an investigation against Cancer Care after unencrypted backup tapes containing electronic protected health information ("ePHI") were stolen from a Cancer Care workforce member's car. OCR's investigation found that Cancer Care failed to: (i) conduct an enterprise-wide risk analysis of the potential for unauthorized access to this protected ePHI; and (ii) implement policies to address the removal of electronic media containing ePHI from the practice location, even though doing so was a common practice within the organization. In addition to paying the settlement amount of $750,000, Cancer Care agreed to a three-year corrective action plan, which requires it to conduct an accurate and thorough

[4] *See* 45 C.F.R. § 160.103 (a "business associate" is any person who "creates, receives, maintains or transmits" PHI on behalf of a covered entity, or provides certain services to a covered entity, which involve the disclosure of PHI to the person).

risk analysis, implement a risk management plan, and review and revise their HIPAA policies and procedures and training program.

OCR's Audit Program

After launching last summer, the second phase of OCR's active audit program of covered entities is well underway ("Phase 2"). Although OCR has indicated that the primary goal of the audits is to learn more about the areas where HIPAA covered entities still struggle to comply, OCR has not ruled out its use of these audits for enforcement purposes. In July, OCR notified 166 covered entities that they had been selected for the Phase 2 desk audits. These covered entities only had ten business days to provide the information requested by OCR without any right to provide supplemental information.

OCR has provided extensive information on its website about the audit process, including the HIPAA provisions that will be covered by the desk audits.[5] Specifically, on the privacy side, selected covered entities must submit evidence of compliance with the Notice of Privacy Practices provision and the Privacy Rule's provision that grants an individual a right to access his or her PHI. With respect to the Security Rule, covered entities must provide evidence of compliance with the security risk analysis and risk management provisions. Finally, for the Breach Notification Rule, OCR requires entities to submit information related to the content and timeliness of HIPAA-mandated notifications to patients and others that the privacy of PHI has been breached. Once OCR completes all of the desk audits, it eventually will conduct a limited number of onsite audits, which will be much more comprehensive and are anticipated to commence later this year. The findings from the initial round of Phase 2 audits will be released by OCR as was done with the results from Phase 1 of the audit program. These findings should serve as a useful tool for all covered entities going forward, regardless of whether they were selected for an audit.

Common Compliance Issues and Recommended Best Practices

OCR's enforcement actions, including those discussed above involving physician group practices, highlight common reoccurring HIPAA compliance issues, including the failure to: (i) have proper written business associate agreements in place; (ii) conduct an accurate and thorough risk analysis of unauthorized disclosures of PHI; and (iii) have appropriate policies and procedures to protect PHI contained in mobile devices. These common HIPAA compliance issues can be addressed through implementation of best practices, some of which are summarized below.

Business Associate Agreements

In addition to the cases involving CCDH and Raleigh Orthopaedic, OCR announced three other settlements with covered entities in the past year that included violations for failing to enter into business associate agreements. The Privacy and Security Rules require that covered entities enter into written agreements with their business associates to ensure that they will appropriately safeguard the covered entity's PHI.[6] If a covered entity is ever subject to an OCR investigation involving such a relationship, OCR will request a copy of the business associate agreement in place between the two entities.

---

[5] *See* HIPAA Privacy, Security, and Breach Notification Audit Program, *available at* https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html (last accessed May 22, 2017).

[6] 45 C.F.R. §§ 164.308(b), 164.314(a), 164.502(e), 164.504(e).

Thus, to avoid potential HIPAA compliance issues involving disclosures of PHI to business associates, and to avoid entering into unnecessary business associate agreements, the following best practices should be implemented:

- Implement written policies and procedures that:
  - Establish a process for identifying whether vendors are business associates for which a business associate agreement is required (e.g., an agreement is necessary if: (i) the person performing the service is not a member of the covered entity's workforce; (ii) the person is performing a service on behalf of the covered entity; and (iii) the service involves creating, receiving, maintaining or transmitting PHI);
  - Designate a responsible individual to ensure business associate agreements are in place prior to disclosing PHI to a business associate and monitor the business associates' compliance with HIPAA and the terms of the business associate agreements; and
  - Establish a process for maintaining business associate agreements for at least six years beyond the termination of a business associate relationship.
- Create a template business associate agreement in accordance with the requirements set forth under HIPAA and a process for negotiating business associate agreements that may be sent by vendors. OCR has provided sample business associate agreement provisions to assist organizations in drafting their agreements.[7] In addition to the provisions that HIPAA explicitly requires, covered entities will also want to reference the underlying service agreement between the parties and include language requiring a business associate to indemnify them for liability for any breaches caused by the business associate.

Risk Analysis and Risk Management

OCR's enforcement actions have also focused on an entity's failure to conduct an accurate and thorough risk analysis to identify and address potential vulnerabilities to ePHI held by the entity. The Security Rule requires entities to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by the organization."[8] A risk analysis is the foundation of an entity's Security Rule compliance program and is the basis for determining what safeguards must be implemented by the entity to ensure the security of its ePHI.

Best practices to consider with respect to risk analysis and risk management include the following:

- Create an inventory of all of the ePHI (including, ePHI located on mobile devices, copiers, services, or medical devices) that is created, received, maintained or transmitted by the entity;
- Perform a risk analysis in accordance with the Security Rule that includes the following:
  - Identification of all potential threats to ePHI, including human, natural and environmental (e.g., hackers, floods, power failures, etc.);

---

[7] *See* Business Associate Contracts, Sample Business Associate Agreement Provisions (published January 25, 2013), *available at* https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html (last accessed May 22, 2017).

[8] 45 C.F.R § 164.308(a)(1)(ii)(A).

- Identification of the various vulnerabilities that a threat could exploit (e.g., a hacker could exploit unpatched software);
- Evaluation of the security measures that have already been implemented;
- Evaluation of the likelihood that a threat will exploit a vulnerability and the impact such may have on the organization (e.g., if a hacker encrypted the data in your EHR and you maintained a current backup of the data, then the impact to your organization would likely be low); and
- Assignment of a risk rating by combining the likelihood and impact (e.g., high, medium or low).[9]

- An entity may want to consider engaging a third party vendor to conduct its risk analysis. If so, there are many vendors in the industry that will perform the risk analysis on a cost-efficient basis. In the event an organization has cybersecurity insurance, the insurance carrier may assist with the cost of the risk analysis and may even require an entity to conduct a risk analysis in order to maintain coverage. However, entities should also be aware that many third party vendors that purport to perform risk analyses actually perform a "gap analysis". A gap analysis typically includes the various provisions of the Security Rule and the security measures an entity has implemented to comply with each provision rather than a full risk analysis as required under the Security Rule. Thus, prior to engaging any third party vendors, ensure that the vendor is experienced and familiar with OCR's guidance on satisfying the risk analysis requirement.[10]
- While the Security Rule does not specify how frequently an entity should conduct a risk analysis, OCR recommends that this type of analysis be evaluated and updated annually, or as needed in response to changes in an entity's environment.[11] For example, if an entity switches to cloud-based storage or new EHR software, it should update its risk analysis to account for any potential risks to ePHI as a result of those technical changes.
- Once an entity has identified the risks to its ePHI, it should implement security measures in order to reduce risks to a reasonable and appropriate level as part of the risk management process. Potential security measures include: firewalls, antivirus software, security training, encryption and patch management. An entity should maintain thorough documentation of any implemented security measures in the event it is subject to an OCR investigation.

Mobile Devices

The theft or loss of mobile devices such as laptops, smart phones and tablets is another common occurrence that causes covered entities to be in breach of HIPAA.

To mitigate HIPAA risks with respect to mobile devices, entities should follow the following best practices:

- Implement a policy that specifically instructs employees and contractors (referred to under HIPAA as "workforce members") on how to safeguard mobile devices containing ePHI and requires workforce members to comply with certain security

[9] Guidance on Risk Analysis Requirements under the HIPAA Security Rule (July 14, 2010), *available at* https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf (last accessed May 22, 2017).
[10] *Id.*
[11] *Id.*

procedures including, for example: use of a password that is changed frequently to access the device, enable a screen lock after the device has not been used for a period of time, install or enable encryption (note: encrypted ePHI is considered "secure" and therefore the theft or loss of an encrypted device is not a reportable breach pursuant to the Breach Notification Rule[12]), install or activate remote wiping or disabling and deleting all ePHI before reusing or discarding a device. The policy should also instruct workforce members to store passwords securely and to refrain from sharing them with others.

- Train workforce members on the policy and document the training.

Conclusion

OCR's HIPAA enforcement activity apparently is not easing up any time soon, so now is the time to evaluate your practice's efforts to meet HIPAA's requirements and make any necessary updates or improvements. In addition to the penalties discussed above, HIPAA breaches can lead to costly private litigation, bad press for the practice, and potential disciplinary action by state licensure boards. Having a robust mechanism for ensuring implementation of HIPAA best practices, including those outlined above, will assist in mitigating your practice's HIPAA compliance risks and, in turn, potentially avoid unnecessary costs and negative publicity associated with an OCR investigation and settlement.

Bonjean is an associate at Polsinelli PC. She counsels physicians, physician practices and hospital clients on HIPAA Privacy and Security compliance and breach response on a national basis. Contact Bonjean at 312.463.6230 or abonjean@polsinelli.com. For more information on Polsinelli's Health Care and Health Care Innovation Practice, visit: http://www.polsinelli.com/services/healthcare http://www.polsinelli.com/services/health-care-innovation.

[12] 45 C.F.R. § 164.402.