HIPAA COMPLIANCE:
A Common Sense Approach

BY DONNA VANDERPOOL, MBA, JD
Ms. Vanderpool is Vice President at PRMS, Inc. in Arlington, Virginia.

Innov Clin Neurosci. 2019;16(1–2):38–41

This ongoing column is dedicated to providing information to our readers on managing legal risks associated with medical practice. We invite questions from our readers. The answers are provided by PRMS, Inc. (www.prms.com), a manager of medical professional liability insurance programs with services that include risk management consultation, education and onsite risk management audits, and other resources to healthcare providers to help improve patient outcomes and reduce professional liability risk. The answers published in this column represent those of only one risk management consulting company. Other risk management consulting companies or insurance carriers may provide different advice, and readers should take this into consideration. The information in this column does not constitute legal advice. For legal advice, contact your personal attorney. Note: The information and recommendations in this article are applicable to physicians and other healthcare professionals so "clinician" is used to indicate all treatment team members.

QUESTION

I hear about breaches of medical privacy and Health Insurance Portability and Accountability Act of 1996 (HIPAA) fines nearly every day. These breaches typically involve large organizations, presumably with large information technology (IT) staffs. I am a psychiatrist in solo practice with part-time front desk staff. I take my professional obligation to protect patient confidentiality seriously but often wonder how I can be expected to be held to the same standard as large organizations with all of their resources.

ANSWER

You bring up a valid point. Here are a few things keep in mind:

✓ **Are you even covered by HIPAA?** Coverage under HIPAA is triggered by specific transactions with health plans done electronically. Only "covered entities" are required to comply with HIPAA and thus are subject to the government's enforcement of HIPAA. See Figure 1 and my prior article[1] for more information on HIPAA's applicability. However, even the entities that are not covered can have liability exposure for breach of confidentiality under the criminal provisions of HIPAA as well as under state law.

✓ **The Security Rule is scalable.** The United States Department of Health and Human Services (HHS), responsible for HIPAA enforcement through its Office for Civil Rights (OCR), has stated that the Security Rule, covering electronic protected health information (ePHI), is scalable. (Note that the privacy rules cover all protected health information [PHI] verbal, paper, or electronic.) What the government might expect a large hospital system to do could differ from what a solo practitioner might be expected to do. HHS has stated that "...the Security Rule is designed to be flexible and scalable so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risk to consumers' ePHI."[2]

✓ **No amount of IT resources can prevent breaches involving blatant violations of patient confidentiality.** Examples of recent HIPAA enforcement actions include:

- *Allowing the filming of television shows in hospitals without patient*

FUNDING: No funding was provided for the preparation of this article.
DISCLOSURES: The author is an employee of PRMS Inc., a risk management consulting company for healthcare providers.
CORRESPONDENCE: Donna Vanderpool, JD; Email: vanderpool@prms.com

authorization. In 2016, a New York hospital entered into a settlement agreement[3] with OCR for $2.2 million for allowing ABC to film a television series "NY Med" in the hospital's emergency department without the authorization of patients involved in the filming. The hospital was also sued by a patient's family member who was horrified to see the death of their loved one on the show. Remarkably, two years later, three Boston hospitals entered a separate resolution agreement[4] with OCR for $999,000. These hospitals also violated HIPAA by allowing television film crews on premises to film another ABC series, "Boston Med," without patient authorization.

- *Allowing pharmaceutical sales representatives access to patient charts*. A physician was arrested for, among other things, allowing drug reps to access patient charts and lying to federal investigators. The physician was convicted[5] of one count of violating HIPAA and one count of obstructing an investigation.

- *Releasing patient information to a reporter without authorization*. A physician's patient contacted a local television station to discuss a dispute with the physician. The reporter then contacted the physician for comment. The privacy officer of the physician's practice instructed the physician to either not respond or respond with "no comment." Instead, the physician spoke with the reporter and impermissibly disclosed the patient's PHI. After OCR investigated and found that the practice had failed to take any disciplinary action against the physician, the practice settled with OCR for $125,000.[6]

- *Failing to terminate an ex-employee's access to PHI*. A hospital failed to terminate remote access to the web-based scheduling calendar, which contained ePHI. OCR's investigation found that the ex-employee had accessed PHI of 557 patients. The investigation also found that there was no business associate agreement between the hospital and the web-based calendar vendor, as required by HIPAA. The hospital paid over $111,000 as part of its resolution agreement with OCR.[7]

- *Sending human immunodeficiency virus (HIV) information to a patient's employer without patient authorization*. A patient who had received HIV treatment from a facility submitted an authorization form from his office fax, directing records to be mailed to his home address or his personal P.O. box. Instead of doing as authorized, the facility staff faxed the complete medical record to the patient's employer. The patient complained to OCR. OCR investigated and found that the same facility was responsible for a different patient's medical record being impermissibly disclosed months prior, but had failed to address the vulnerabilities to prevent further breaches. The facility paid $387,000 to settle the case with OCR[8] and was sued by the patient, who alleged negligence and negligent infliction of distress under state law.

✓ **Criminals are interested in getting PHI.** Reports of using malware to hold a provider's ePHI for ransom are frequent. For more information on ransomware, see HHS's "Fact Sheet: Ransomware and HIPAA".[9] While there are many ways for criminals to access systems with ePHI, one way at which they are particularly proficient is phishing, or the fraudulent practice of sending emails purporting to be from a reputable company to obtain personal information. Anthem, a larage insurance company, paid OCR $16 million in a record HIPAA settlement[10] following the largest United States health data breach in history. PHI of close to 79 million individuals, including names and social security numbers, was stolen by cyber attackers. The criminals infiltrated Anthem's system through spear phishing emails; at least one employee responded to a malicious email and opened the door to further attacks. In addition to impermissible disclosure of ePHI, OCR found other violations, including a failure to conduct an enterprise-wide risk analysis. OCR has developed specific guidance on phishing attacks[11] and cyber security,[12] including advice for small healthcare providers.

FIVE KEY ACTIONS TO STAY HIPAA COMPLIANT

1 **Perform the HIPAA-required risk analysis—and review and update periodically.** In one case, a network of medical providers paid $3.5 million to OCR in settlement[13] after reporting five breaches to OCR. Upon investigation, OCR found a failure to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of its ePHI. (For resources, see the HIPAA Checklist.)

2 **Train all employees on HIPAA's requirements, your policies and procedures, and the potential for harmful phishing emails.** Document the initial and annual training, and consider having employees sign confidentiality agreements.

3 **Ensure you have business associateagreements (BAAs) from all of your business associates (BAs).** HHS describes a BA as "a person or entity other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information."[14] Examples include, but are not limited to, answering services, billing services, and transcription services. Covered entities are required to enter into agreements

FIGURE 1. HIPAA COMPLIANCE CHECKLIST

1. Are you a "Covered Entity" under HIPAA?

A. If yes—You are responsible for complying with the federal HIPAA and HITECH laws, as well as state confidentiality law. Continue answering the questions below.

B. If no—You must comply with state confidentiality law. Additionally, it is suggested that you review the questions below as the Privacy and Security Rules are floors of confidentiality protection, and, as a psychiatrist, you are held to a much higher legal and ethical standards from protection of patient information.

C. If you do not know—HHS (the Department of Health and Human Services), responsible for enforcement of the Privacy and Security Rules, has created the following resources to assist you in determining whether you are a Covered Entity:

i. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

ii. http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf

2. Do you have your Privacy Rule policies and procedures documented?

A. Summary of the Privacy Rule from HHS: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

B. PRMS resource: In the HIPAA Help section of our website (https://www.prms.com/services/risk-management/hipaa-help/), we provide checklists that might assist you in drafting policies as well as model forms (from 2003)

3. Do you have your Notice of Privacy Practices?

Model from HHS: http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/

4. Are your Privacy Rule policies and procedures being followed?

A. Are patients actually receiving your Notice of Privacy Practices?

B. Are all requests for restrictions considered?

C. Are access and amendment requests handled timely?

D. Is only the minimum necessary amount of protected health information (PHI) being released unless the patient has authorized release of the entire record?

5. Do you have your Security Rule policies and procedures documented?

A. Summary of the Security Rule from HHS: http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

B. Guidance on compliance from HHS: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

C. PRMS resource: Security Rule Compliance Checklist with Resources for Small Practices, available in the HIPAA Help section of our website (https://www.prms.com/services/risk-management/hipaa-help/)

6. Are your Security Rule policies and procedures being followed?

A. Are all of your computers with PHI password-protected?

B. Are all of your portable devices with PHI, such as laptops and tablets, encrypted?

C. Are all of your electronic devices containing PHI, including copiers, stripped of all PHI prior to disposal, sale, or return to vendor?

i. See HHS's recommended resource, FTC's Copier Data Security at http://business.ftc.gov/documents/bus43-copier-data-security

ii. See $1.2 million enforcement action against a Covered Entity for failing to remove PHI from a copier at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/affinity-agreement.html

D. Are the other required elements being met?

7. Have you done your risk assessment—initially and on-going?

A. From HHS: Risk Assessment Guidance, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalintro.html

B. From HHS: Security Risk Assessment (SRA) tool, www.hhs.gov/news/press/2014pres/03/20140328a.html

C. To learn of risks that are the subject of HHS' enforcement, subscribe to OCR's listserv: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/listserv.html

8. Do you understand the requirements of the Breach Notification Rule?

Resources from HHS: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

9. Are your Breach Notification Rule policies and procedures being followed:

A. Can all employees identify a breach?

B. Do employees understand that all possible breaches must be reported to you as soon as possible?

C. Do you call your personal attorney immediately upon learning of a potential breach of PHI?

10. Have your employees signed confidentiality agreements?

A model confidentiality agreement is available on the PRMS website. (https://www.prms.com)

11. Have you provided yearly HIPAA training to staff?

HHS's online HIPAA training courses (with CME) are available to all through Medscape: http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/index.html

12. Are your training records documented?

13. Do your employees understand the training?

A. Is PHI being properly maintained at workstations?

B. How is PHI actually being disposed of?

C. Is PHI only be accessed and disclosed pursuant to authorization, legal mandate, or exception to confidentiality?

D. Does staff understand that merely not mentioning identifying information does not mean confidentiality is being maintained?

E. Are computers positioned so that patients cannot read the screens?

14. Are you prepared for a HIPAA audit?

HHS's HIPAA Audit Protocol: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

15. Do you have business associate agreements (BAAs) from all of your business associates (BAs)?

A. BAs are third parties that perform a function on behalf of or provide services to a Covered Entity that require the release of PHI. Note: PRMS is a BA of any program participant that is a Covered Entity under HIPAA. Our BAA is available on our website for download: https://www.prms.com/media/1323/businessagreement.pdf

C. HHS's Sample BAA Provisions: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

D. Have all BAs provided you with BAAs?

16. Are you aware that, aside from criminal penalties, civil penalties for HIPAA violations can be as much as $50,000 per incident with a yearly cap of $1.5 million for multiple identical violations?

17. Are you familiar with HHS's enforcement actions?

Case examples and resolution agreements are available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.

18. Are your employees prohibited from removing PHI (paper or electronic) from the office?

19. If you have PHI on mobile devices, such as a laptop or tablet, is the device encrypted?

HHS's educational materials on privacy and security with mobile devices: http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

(BAAs) with BAs to ensure that the BA will appropriately safeguard PHI. One physician group had to pay $500,000 to settle an OCR investigation[15] that found the group failed to have a BAA with the group's billing service.

4 **Protect all PHI, including special protections for ePHI.** OCR expects all portable devices with ePHI, such as cell phones and laptops, to be appropriately encrypted. OCR investigated a Texas health system following three data breach reports involving the theft of an unencrypted laptop from an employee's home and the loss of two USB drives containing the unencrypted ePHI of more than 33,500 individuals. The covered entity was ordered to pay $4.3 million in penalties.[16] Other actions that protect ePHI include backing up ePHI appropriately and ensuring firewalls and anti-virus protections are up to date.[9]

5 **If you think there has been a breach of confidentiality, contact your risk manager or medical malpractice insurance carrier.** Your insurance policy might include coverage related to HIPAA and other confidentiality violations.

REFERENCES

1. Vanderpool D. HIPAA—Should I be Worried? *Innov Clin Neurosci*. 2012;9(11–12):51–55.
2. United States Department of Health & Human Services site. Summary of the HIPAA Security Rule. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html. Accessed 6 Feb 2019.
3. United States Department of Health & Human Services site. Unauthorized filming for "NY Med" results in $2.2 million settlement with New York Presbyterian Hospital. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/new-york-presbyterian-hospital/index.html. Accessed 6 Feb 2019.
4. United States Department of Health & Human Services site. Unauthorized disclosure of patients' protected health information during ABC television filming results in multiple HIPAA settlements totaling $999,000. https://www.hhs.gov/about/news/2018/09/20/unauthorized-disclosure-patients-protected-health-information-during-abc-filming.html. Accessed 6 Feb 2019.
5. United States Department of Justice. Springfield doctor convicted by jury of illegally sharing patient medical files. https://www.justice.gov/usao-ma/pr/springfield-doctor-convicted-jury-illegally-sharing-patient-medical-files. Accessed 6 Feb 2019.
6. United States Department of Health & Human Services site. Allergy practice pays $125,000 to settle doctor's disclosure of patient information to a reporter. https://bit.ly/2Gr83Tr. Accessed 6 Feb 2019.
7. U.S. Department of Health & Human Services site. Colorado hospital failed to terminate former employee's access to electronic protected health information. https://bit.ly/2HUMzR2. Accessed 6 February 2019.
8. U.S. Department of Health & Human Services site. Careless handling of HIV information jeopardizes patient's privacy, costs entity $387k. https://www.hhs.gov/about/news/2017/05/23/careless-handling-hiv-information-costs-entity.html. Accessed 6 February 2019.
8. U.S. Department of Health & Human Services. FACT SHEET: Ransomware and HIPAA. https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf. Accessed 6 February 2019.
9. U.S. Department of Health & Human Services site. Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History. https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html. Accessed 6 February 2019.
10. U.S. Department of Health & Human Services. Phishing. https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-february-2018.pdf Accessed 6 February 2019.
11 . U.S. Department of Health & Human Services site. Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx. Accessed 6 February 2019.
12. U.S. Department of Health & Human Services site. Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules https://www.hhs.gov/about/news/2018/02/01/five-breaches-add-millions-settlement-costs-entity-failed-heed-hipaa-s-risk-analysis-and-risk.html Accessed 6 February 2019.
13. U.S. Department of Health & Human Services site. Business Associate Contracts. Sample business associate agreement provisions https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html. Accessed 6 February 2019.
14. U.S. Department of Health & Human Services site. Florida contractor physicians' group shares protected health information with unknown vendor without a business associate agreement. https://bit.ly/2HUNj8M. Accessed 6 February 2019.
15. U.S. Department of Health & Human Services site. Judge rules in favor of OCR and requires a Texas cancer center to pay $4.3 million in penalties for HIPAA violations. https://bit.ly/2DXc9kI. Accessed 6 February 2019. ICNS