Top Five HIPAA Lessons Learned: A Review of HHS Resolution Agreements

by JUSTIN POPE, JD
Mr. Pope is an Associate Risk Manager at Professional Risk Management Services (PRMS).

Innov Clin Neurosci. 2020;17(7–9):45–48

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 on-site risk management audits, and other resources offered to health care 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 might 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 health care professionals so "clinician" is used to indicate all treatment team members.

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 health care providers.

CORRESPONDENCE: Justin Pope, JD; Email: jpope@prms.com

QUESTION:
I noticed the United States (US) Department of Health and Human Services (HHS) posts Health Insurance Portability and Accountability Act (HIPAA) cases on their website. There are quite a few cases listed, and I haven't yet had the chance to review them. Have you observed any enforcement trends that might be helpful?

ANSWER:

Yes. After reviewing the US HHS's Office of Civil Rights (OCR) case resolution agreements, there are at least five lessons to be learned. It should also be noted that OCR's enforcement has not slowed during the pandemic.

ENFORCEMENT

OCR resolves most cases that fall within its jurisdiction informally by accepting voluntary compliance, corrective actions (adopted obligations), and/or resolution agreements (monetary settlements). If OCR cannot resolve the matter informally, civil money penalties may be enforced.[1]

While this article will focus on federal civil enforcement cases, there could always be the potential for federal criminal enforcement, state criminal enforcement, and state civil enforcement.

TOP FIVE LESSONS LEARNED

1 **A thorough, accurate, and current risk assessment is essential.** When investigating covered entities for potential HIPAA violations, OCR has often found that the covered entity failed to conduct a "thorough and accurate" risk assessment. HIPAA's Security Rule requires covered entities to assess their risk, weighing potential threats and vulnerabilities and implementing policies and procedures accordingly.[2] For example, have you determined what type of protected health information (PHI) you store and the manner in which you store it? Do you know who has access to your PHI? Do you track access in any meaningful way?

Security Rule requirements are scalable and flexible, and they allow covered entities to comply in a manner consistent with the complexity of their particular operations and circumstances. It is understood that small providers and solo practices are less likely to have information technology (IT) departments, meaning their approach to compliance will be much different from a large healthcare system.[3] However, the most important thing is that a covered entity of any size can show it has thoughtfully and carefully considered security risks to PHI and taken reasonable measures to minimize or nullify those risks.

Notable enforcement resolutions include:

- **North Memorial Health Care**, a not-for-profit healthcare system in Minnesota, agreed to a monetary payment of $1,550,000 and a corrective action plan after reporting an unencrypted laptop that contained the electronic protected health information of approximately 9,497 individuals had been stolen from a business associate's vehicle. Not only did North Memorial provide Accretive, a business associate, with access to North Memorial's unencrypted laptop containing

electronic protected health information (ePHI) before first obtaining a written business associate agreement, but North Memorial failed to conduct an accurate and thorough risk analysis that took into account all of North Memorial's IT equipment, applications, and data systems using ePHI.[4]

- **The University of Washington Medicine (UWM)** agreed to a settlement including a monetary payment of $750,000, a corrective action plan, and annual reports on the organization's compliance efforts. According to OCR's investigation in November 2013, the ePHI of approximately 90,000 individuals had been accessed after an employee downloaded an email attachment that contained malicious malware. OCR found that UWM had not ensured all of its affiliated entities were properly conducting risk assessments and appropriately responding to the potential risks and vulnerabilities in their respective environments.[5]

Additional resources include:

- **The Final Guidance on Risk Analysis:** https://www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html
- **Security Risk Assessment (SRA) Tool:** https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
- **Security Rule Guidance Material:** https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

2 Devices storing electronic protected health information (ePHI) should be encrypted and password-protected.

This is a lesson that should have been learned quite some time ago. Over a third of OCR's case resolution agreements have involved the theft or loss of unencrypted portable devices storing PHI. While the inability to safeguard devices in these cases is alarming, even more troubling is the fact that covered entities still fail to encrypt their portable devices.

HHS excludes any unauthorized disclosure from the definition of "breach" if the recipient would not be able to retain that information. Although encryption is not required by the Security Rule, it acts as a safe harbor. The presumption is that a lost, but encrypted device cannot be accessed, and therefore, does not constitute a breach.[6] Many of these settlements could have potentially been avoided by encrypting mobile devices, and OCR has been vocal about the protection encryption offers.

Notable Enforcement Resolutions include:

- **Lifespan Health System**, a nonprofit health system based in Rhode Island, agreed to pay $1,040,000 to OCR and implement a corrective action plan. In February 2017, an employee's car was broken into while it was parked in a public lot. An unencrypted laptop used by the employee for work purposes was stolen and never recovered. Lifespan determined that the employee's emails might have been cached on the device's hard drive. An analysis revealed the thieves had access to: patient names, medical record numbers, demographic information, including partial address information, and the name of one or more medications that were prescribed or administered to patients.[7]
- **The University of Rochester Medical Center (URMC)** paid $3 million to settle an investigation involving unencrypted mobile devices. In 2013, URMC reported an unencrypted flash drive containing ePHI had been lost. In 2017, URMC reported that an unencrypted personal laptop belonging to one of its resident surgeons was stolen from a treatment facility. OCR noted it had already closed a similar investigation in 2010, involving a lost unencrypted flash drive after technical assistance was provided. Despite the previous investigation, the covered entity had not implemented an encryption policy or, alternatively, documented why encryption was not reasonable and appropriate to safeguard ePHI.[8]
- **Feinstein Institute for Medical Research (FIMR)** agreed to pay OCR $3.9 million and undertook a corrective action plan to settle potential HIPAA violations. In September 2012, FIMR reported that an unencrypted laptop was stolen from the car of one of its employees. After investigating, HHS found that FIMR impermissibly disclosed the ePHI of 13,000 individuals when the FIMR-owned laptop computer was stolen.[9]

Additional resources include:

- **Breach Notification Rule (see Unsecured Protected Health Information and Guidance:** https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- **Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals:** https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html
- **Guide to Storage Encryption for End User Devices:** https://www.hhs.gov/sites/default/files/nist800111.pdf

3 Get the Business Associate Agreement!

A "business associate" is a third party, outside of a covered entity's workforce, who provides certain services to a covered entity necessitating access to protected health information. Under HIPAA, if you are a covered entity, you must ensure that there is a Business Associate Agreement (BAA) in place with the third party who will have access to your patient information. Under this agreement, the business associate agrees to maintain the confidentiality, security, and integrity of your patients' records. Covered entities are required to have such an agreement in place before disclosing any PHI to a business associate, or else they risk making an impermissible disclosure.[10]

Notable enforcement resolutions include:

- **Advanced Care Hospitalists PL** agreed to pay $500,000 to OCR and adopt a corrective action plan to settle potential HIPAA violations. Advanced Care provides contracted internal medicine physicians to hospitals and nursing homes in west central Florida. In 2011, Advanced Care contracted

with an individual for medical billing services. Although he appeared to be representing Doctor's First Choice Billings, the individual provided billing services without the owner's permission. Eventually, Advanced Care was notified that the PHI of over 9,000 individuals had been publicly viewable on First Choice's website. Upon investigation, OCR found patient information had been improperly disclosed to First Choice as the two parties had never entered into a BAA.[11]

- **The Center for Children's Digestive Health (CCDH)** paid HHS $31,000 to settle potential HIPAA violations and agreed to a corrective action plan. CCDH is a small, pediatric healthcare provider that operates in Illinois. HHS began an investigation of business associate, FileFax, Inc., which stored records containing protected health information for CCDH. Although CCDH began disclosing PHI to Filefax in 2003, neither party could produce a signed BAA prior to Oct. 12, 2015.[12]
- **Pagosa Springs Medical Center**, a critical access hospital, agreed to pay $111,400 to OCR and adopt a corrective action plan to settle potential HIPAA violations. In addition to other violations, OCR found that Pagosa had impermissibly disclosed the ePHI of at least 557 to a web-based scheduling calendar vendor without a first having a BAA in place.[13]

Additional resources include:

- **HHS Business Associate Guidance:** https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html
- **HHS Business Associate Sample Provisions:** https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html
- **Direct Liability of Business Associates:** https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html

4 Covered entities are responsible for the actions of their employees. In many case resolutions, covered entities were held responsible for the actions of their employees. For this reason, providers and office managers must be vigilant and proactive when addressing compliance issues. Per OCR, "Covered entities are responsible for the actions of their employees. This is why it is vital that trainings and meaningful policies and procedures, including audit trails, become part of the everyday operations of any healthcare provider."[14]

Notable enforcement resolutions include:

- **St. Luke's-Roosevelt Hospital Center Inc.** agreed to pay $387,200 and adopt a comprehensive corrective action plan to settle potential HIPAA violations related to an impermissible disclosure. In 2014, OCR found that a staff member had impermissibly faxed a patient's PHI to his employer rather than sending it to the requested personal post office box. OCR also discovered that a similar incident had occurred nine months prior and appropriate steps to remedy the problem were not taken. Per the corrective action plan, OCR required all members of the workforce to complete training and that all training materials be submitted for review.[15]
- **Memorial Healthcare System (MHS)** paid $5.5 million to settle potential HIPAA violations and agreed to a robust corrective action plan. MHS is a nonprofit corporation that operates healthcare facilities throughout the South Florida area. A former employee's login credentials were used to access ePHI maintained by MHS on a daily basis without detection from April 2011 to April 2012, affecting 80,000 individuals. Although it had workforce access policies and procedures in place, MHS failed to regularly review and terminate users' right of access despite having identified this risk during several risk assessments.[16]
- **The University of California at Los Angeles Health System** agreed to settle potential HIPAA violations for $865,500 and committed to a corrective action plan. The agreement resolved two complaints alleging that unauthorized employees repeatedly looked at the ePHI of celebrity patients from 2005 to 2008 without a valid reason. Through policies and procedures covered entities are required to restrict PHI access to only those employees necessary.[17]

Additional resources include:

- **HHS Training Resources:** https://www.hhs.gov/hipaa/for-professionals/training/index.html
- **The Office of the National Coordinator for Health Information Technology's Privacy and Security Games:** https://www.healthit.gov/topic/privacy-security-and-hipaa/privacy-security-training-games

5 HIPAA compliance is an ongoing, dynamic process. OCR's enforcement activity makes it quite clear that it's not enough to simply have drafted HIPAA policies and procedures. HIPAA compliance requires ongoing assessment. Policies that might be reasonable today might not be reasonable tomorrow. Much like clinical and financial considerations, the privacy and security of patient information should be taken into account when determining how to establish a new policy or utilize a new technology in the office. Routinely making HIPAA a part of the discussion goes a long way toward reducing your exposure.

Notable enforcement decisions:

- **Woman & Infants Hospital of Rhode Island** agreed to pay $400,000 and adopt a correct action plan to settle a breach of its unsecured ePHI. OCR commenced an investigation after the hospital reported that unencrypted backup tapes at two of its facilities were missing. While investigating, OCR cited the hospital for failing to update a BAA in accordance with the recently published Omnibus Rule requirements. As a result, any information that had been provided to the business associate after the date of noncompliance was deemed an impermissible disclosure. This case highlights the importance of

reviewing and updating documents and policies.[18]

- **Anchorage Community Mental Health Services (ACMHS)** agreed to pay $150,000 to OCR for potential HIPAA violations. OCR opened an investigation after it was notified of a breach of ePHI affecting 2,743 patients. During the investigation, OCR found that even though ACMHS introduced sample policies and procedures in 2005, they were no longer being followed at the time of the breach. ACMHS had also failed to update IT guidance and continued to use outdated software.[19]

CONCLUSION

The threat of HIPAA enforcement exists for healthcare organizations both large and small and should not be taken lightly. OCR continues to enforce HIPAA violations and announce case resolution agreements, even during the pandemic. To avoid enforcement action, covered entities should be proactive about the confidentiality and security of health information and mindful of the top five lessons identified in this article.

REFERENCES

1. United States Department of Health & Human Services site. How OCR enforces the HIPAA Privacy & Security Rules. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html. Accessed 3 Aug 2020.
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 3 Aug 2020.
3. United States Department of Health & Human Services site. HIPAA Security Series. 7 Security Standards: Implementation for the Small Provider. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf?language=es. Accessed 3 Aug 2020.
4. United States Department of Health & Human Services site. $1.55 Million Settlement Underscores the Importance of Executing HIPAA Business Associate Agreements. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/north-memorial-health-care/index.html. Accessed 3 Aug 2020.
5. United States Department of Health & Human Services site. $750,000 HIPAA Settlement Underscores the Need for Organization-Wide Risk Analysis. https://wayback.archive-it.org/3926/20170127185458/https://www.hhs.gov/about/news/2015/12/14/750000-hipaa-settlement-underscores-need-for-organization-wide-risk-analysis.html. Accessed 3 Aug 2020.
6. United States Department of Health & Human Services site. Breach Notification Rule. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html. Accessed 3 Aug 2020.
7. United States Department of Health & Human Services site. Lifespan Pays $1,040,000 to OCR to Settle Unencrypted Stolen Laptop Breach. https://www.hhs.gov/about/news/2020/07/27/lifespan-pays-1040000-ocr-settle-unencrypted-stolen-laptop-breach.html. Accessed 3 Aug 2020.
8. United States Department of Health & Human Services site. Failure to Encrypt Mobile Devices Leads to $3 Million HIPAA Settlement. https://www.hhs.gov/about/news/2019/11/05/failure-to-encrypt-mobile-devices-leads-to-3-million-dollar-hipaa-settlement.html. Accessed 3 Aug 2020.
9. United States Department of Health & Human Services site. Improper Disclosure of Research Participants' Protected Health Information Results in $3.9 Million HIPAA Settlement. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/feinstein/index.html. Accessed 3 Aug 2020.
10. United States Department of Health & Human Services site. Business Associates. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html. Accessed 3 Aug 2020.
11. United States Department of Health & Human Services site. Florida Contractor Physicians' Group Shares Protected Health Information with Unknown Vendor Without a Business Associate Agreement. https://www.hhs.gov/about/news/2018/12/04/florida-contractor-physicians-group-shares-protected-health-information-unknown-vendor-without.html. Accessed 3 Aug 2020.
12. United States Department of Health & Human Services site. No Business Associate Agreement? $31K Mistake – April 20, 2017. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ccdh/index.html. Accessed 4 Aug 2020.
13. United States Department of Health & Human Services site. Colorado Hospital Failed to Terminate Former Employee's Access to Electronic Protected Health Information. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/pagosasprings/index.html. Accessed 4 Aug 2020.
14. United States Department of Health & Human Services site. UCLA Health System Settle Potential Violations of the HIPAA Privacy and Security Rules. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/ucla-health-system/index.html. Accessed 4 Aug 2020.
15. United States 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 4 Aug 2020.
16. United States Department of Health & Human Services site. $5.5 Million HIPAA Settlement Shines Light on the Importance of Audit Controls. https://www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html#:~:text=Memorial%20Healthcare%20System%20(MHS)%20has,a%20robust%20corrective%20action%20plan. Accessed 4 Aug 2020.
17. United States Department of Health & Human Services site. UCLA Health System Settle Potential Violations of the HIPAA Privacy and Security Rules. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/ucla-health-system/index.html. Accessed 4 Aug 2020.
18. United States Department of Health & Human Services site. HIPAA Settlement Illustrates the Importance of Reviewing and Updating, as Necessary, Business Associate Agreements – September 23, 2016. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/wih/index.html. Accessed 4 Aug 2020.
19. United States Department of Health & Human Services site. HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/acmhs/index.html. Accessed 4 Aug 2020. ICNS