October 2023 OCR Cybersecurity Newsletter

How Sanction Policies Can Support HIPAA Compliance

Last year, the Department of Health and Human Services' (HHS) Health Sector Cybersecurity Coordination Center (HC3) released a threat brief on the different types of social engineering[1] that hackers use to gain access to healthcare information systems and data.[2] The threat brief recommended several protective measures to combat social engineering, one of which was holding "every department accountable for security." An organization's sanction policies can be an important tool for supporting accountability and improving cybersecurity and data protection. Sanction policies can be used to address the intentional actions of malicious insiders, such as the stealing of data by identity-theft rings, as well as workforce member failures to comply with policies and procedures, such as failing to secure data on a network server or investigate a potential security incident.

The HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") require covered entities and business associates ("regulated entities") to ensure that workforce members[3] comply with the HIPAA Rules. Regulated entities are responsible for protecting the privacy and security of protected health information (PHI)[4] by training their workforce,

adopting written policies and procedures, and sanctioning workforce members who violate those policies and procedures.[5] Sanction policies are specifically required by both the Privacy Rule and the Security Rule:

- The Privacy Rule requires covered entities[6] to "have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of [the Privacy Rule] or [the Breach Notification Rule] of this part."[7]
- The Security Rule requires covered entities and business associates to: "[a]pply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate."[8]

I. The Functions of a Sanction Policy

Sanction policies can improve a regulated entity's compliance with the HIPAA Rules.[9] Imposing consequences on workforce members who violate a regulated entity's policies or the HIPAA Rules can be effective in creating a culture of HIPAA compliance and improved cybersecurity because of the knowledge that there is "a negative consequence to noncompliance enhances the likelihood of compliance."[10] Training workforce members on a regulated entity's sanction policy can also promote compliance and greater cybersecurity vigilance by informing workforce members in advance which "actions are prohibited and punishable."[11] A sanction policy that clearly communicates a regulated entity's expectations should ensure that workforce members understand their individual compliance obligations and consequences of noncompliance.

II. Content: What Should a Sanction Policy Look Like?

Because HIPAA regulated entities "are so varied in terms of installed technology, size, resources, and relative risk,"[12] the HIPAA Rules allow for a flexibility of approach to achieve compliance. This flexibility of approach also extends to sanction policies: the Privacy Rule preamble states that "we leave the details of sanction policies to the discretion of the covered entity . . . [that] will be familiar with the circumstances of the violation . . . ."[13] Similarly, the Security Rule preamble states that regulated entities "have the flexibility to implement the standard in a manner consistent with numerous factors, including such things as, but not limited to, their size, degree of risk, and environment."[14]

The HIPAA Rules do not require regulated entities to impose any specific penalty for any individual violation, or to implement any particular sanction methodology. Rather, in any individual case "[t]he type and severity of sanctions imposed, and for what causes, must be determined by each covered entity [or business associate] based upon its security policy and the relative severity of the violation."[15] Regulated entities may structure their sanction policies in the manner most suitable to their organization. Regulated entities may want to consider the following when drafting or revising their sanction policies:

1. Documenting or implementing sanction policies pursuant to a formal process.[16]
2. Requiring workforce members to affirmatively acknowledge that a violation of the organization's HIPAA policies or procedures may result in sanctions.[17]
3. Documenting the sanction process, including the personnel involved, the procedural steps, the time-period, the reason for the sanction(s), and the final outcome of an investigation. NOTE: These records should be retained for at least six years.[18]
4. Creating sanctions that are "appropriate to the nature of the violation."[19]
5. Creating sanctions that "vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicated a pattern or practice of improper use or disclosure of protected health information."[20]
6. Creating sanctions that "range from a warning to termination."[21]
7. Providing examples "of potential violations of policy and procedures."[22]

By making these considerations, regulated entities can craft a thoughtful and well-documented sanction policy that informs workforce members of the regulated entity's expectations, deters misconduct, and promotes HIPAA compliance through greater understanding and transparency of the policies and procedures that protect the privacy and security of PHI.

III. **Execution: Sanctioning Consistently**

How a regulated entity implements its sanction policy is just as important as the policy's content. It is important for a regulated entity to consider whether its sanction policies align with its general disciplinary policies, and how the individuals or departments

involved in the sanction processes can work in concert, when appropriate. Regulated entities may also want to consider how sanction policies can be fairly and consistently applied throughout the organization, to all workforce members, including management. Indeed, sanctioning workforce members inconsistently can undermine the integrity of a regulated entity's compliance program.[23]

In 2017 and 2018, OCR resolved two investigations with regulated entities that potentially violated the HIPAA Rules sanctions requirements. In the first case, OCR found evidence that the regulated entity potentially "impermissibly disclosed the patient's PHI through press releases issued to fifteen media outlets and/or reporters," and senior leaders disclosed the patient's PHI to advocacy groups and in a published statement on their website. OCR also found evidence that the regulated entity potentially "failed to document timely the sanctions imposed against members of its workforce who failed to comply with its privacy policies and procedures or the Privacy Rule."[24] In the second case, OCR found evidence of a potential violation of the sanction requirements when a workforce member allegedly disclosed PHI to a reporter, and then the regulated entity allegedly failed to apply appropriate sanctions against its Workforce Member who failed to comply with the entity's privacy policies and procedures and the Privacy Rule."[25]

IV. **Conclusion**

Sanction policies offer a great opportunity for regulated entities to establish and communicate compliance obligations and expectations to their workforce members. The deterrent effect of penalizing noncompliance and misconduct paired with clear communications about the consequences of noncompliance can promote greater compliance with the HIPAA Rules through accountability, understanding, and transparency. At a time when the need for constant vigilance to protect ePHI is at an all-time high due to hacking and other threats to the privacy and security of health information, regulated entities should make sure that their policies and practices include sanction policies that hold all workforce members accountable for noncompliance with the HIPAA Rules.

Additional Resources

- NIST 800-66 Rev. 1. (4.1.6) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf - PDF <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-66r1.pdf>

- NIST 800-53 Rev. 5. (PS-8) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf - PDF <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r5.pdf>
- HHS HIPAA Security Series - 2: Security Standards - Administrative Safeguards https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf - PDF <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf>
- United States Office of Personnel Management, Managing Federal Employees' Performance Issues or Misconduct https://www.opm.gov/policy-data-oversight/employee-relations/reference-materials/managing-federal-employees-performance-issues-or-misconduct.pdf - PDF <https://www.opm.gov/policy-data-oversight/employee-relations/reference-materials/managing-federal-employees-performance-issues-or-misconduct.pdf>
- United States Office of Personnel Management, Addressing and Resolving Poor Performance: A Guide for Supervisors https://www.opm.gov/policy-data-oversight/employee-relations/employee-rights-appeals/performance-based-actions/toolkit.pdf - PDF <https://www.opm.gov/policy-data-oversight/employee-relations/employee-rights-appeals/performance-based-actions/toolkit.pdf>
- *Douglas v. Veterans Administration*, 5 M.S.P.R. 280 (1981), in which the Merit Systems Protection Board issued a list of criteria that Federal supervisors must consider when determining the appropriate sanction for employee misconduct (the "Douglas Factors"). https://www.opm.gov/policy-data-oversight/employee-relations/reference-materials/douglas-factors.pdf - PDF <https://www.opm.gov/policy-data-oversight/employee-relations/reference-materials/douglas-factors.pdf>

* This document is not a final agency action, does not legally bind persons or entities outside the Federal government, and may be rescinded or modified in the Department's discretion.

Endnotes

[1] "The process of attempting to trick someone into revealing information (e.g., a password)." *See* NIST Information Technology Laboratory, Computer Security Resource Center, Glossary, available at https://csrc.nist.gov/glossary/term/social_engineering <https://csrc.nist.gov/glossary/term/social_engineering>.

[2] Health Sector Cybersecurity Coordination Center, *The Impact of Social Engineering on Healthcare*, August 18, 2022, https://www.hhs.gov/sites/default/files/the-impact-of-social-engineering-on-healthcare.pdf - PDF <https://www.hhs.gov/sites/default/files/the-impact-of-social-engineering-on-healthcare.pdf>.

[3] Under the HIPAA Rules, "*Workforce* means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate." 45 CFR 160.103 (definition of "Workforce").

[4] *See* 45 CFR 160.103 (definition of "Protected Health Information").

[5] 45 CFR 164.530(b), 164.530(e)(1),164.530(i)(1), 164.308(a)(1)(ii)(C), 164.308(a)(5)(i), and 164.316.

[6] The Privacy Rule's sanction requirement applies only to covered entities, not to business associates. *See* OCR guidance *Direct Liability of Business Associates* (https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html>) for more information regarding business associate HIPAA liability.

[7] 45 CFR 164.530(e)(1). Note, this standard does not apply to workforce members' actions that are covered by and meet the protections of 164.502(j) ("disclosures by whistleblowers and workforce member crime victims") and 164.530(g)(2) ("covered entity must refrain from intimidation and retaliation").

[8] 45 CFR 164.308(a)(1)(ii)(C).

[9] Health Insurance Reform: Security Standards; Final Rule 68 FR 8334, 8346 (February 20, 2003) (stating that "[s]ome form of sanction or punishment activity must be instituted for noncompliance. Indeed, we question how the statutory requirement for safeguards 'to ensure compliance by a [covered entity's] officers and employees' could be met without a requirement for a sanction policy.")

[10] *Id.* at 8347.

[11] Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 FR 82462, 82747 (December 28, 2000) (stating that "[w]e believe it is important for the covered entity to have these sanction policies and procedures documented so that employees are aware of what actions are prohibited and punishable . . . employees should be trained to understand the covered entity's expectations and understand the consequences of any violation.")

[12] 68 FR 8335.

[13] 65 FR 82747.

[14] 68 FR 8346.

[15] *Id*. at 8347.

[16] 65 FR 82562 (explaining that "[w]e also require a covered entity to have written policies and procedures for the application of appropriate sanctions for violations of this subpart and to document those sanctions").

[17] *See* HHS HIPAA Security Series - 2: Security Standards - Administrative Safeguards ("Does the organization require employees to sign a statement of adherence to security policy and procedures (*e.g.*, as part of the employee handbook or confidentiality statement) as a prerequisite to employment?")); National Institute of Standards and Technology (NIST) Special Publication 800-66 Rev. 1: *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA*) *Security Rule*, page 18 ("Have employees been made aware of policies concerning sanctions for inappropriate access, use, and disclosure of EPHI?").

[18] *See* HIPAA Audit Protocol ("Elements to review may include but are not limited to: • Personnel involved in the sanction process • Required steps and time period • Notification steps • Reason for the sanction
• Identification of the sanctions applied to compliance failures • Documentation of the sanction outcome") https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html>; and 45 CFR 164.316 and 164.530(e)(2).

[19] 65 FR 82562.

[20] *Id*.

[21] *Id*.

[22] *See* HHS HIPAA Security Series - 2: Security Standards - Administrative Safeguards, https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

[23] 45 CFR 308(a)(1)(ii)(C), 164.530(e)(1). *See also* 65 FR 82747 ("All members of a covered entity's workforce are subject to sanctions for violations").

[24] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/mhhs/index.html <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/mhhs/index.html>

[25] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/allergyassociates/index.html <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/allergyassociates/index.html>.

Content created by Office for Civil Rights (OCR)
Content last reviewed October 18, 2023