Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

Avoiding HIPAA Penalties: A Checklist for Covered Entities

Insight — May 29, 2024

The HIPAA Privacy, Security, and Breach Notification Rules[1] apply to healthcare providers who engage in certain electronic transactions, healthcare clearinghouses, and health plans, including employee group health plans with 50 or more participants or that are administered by a third party.[2] Covered entities must comply with HIPAA for the following reasons:

1. Civil Penalties. The Office for Civil Rights (OCR) may—and in some cases must—impose civil penalties against covered entities and their business associates who violate HIPAA. The following chart summarizes the tiered penalty structure currently in effect; the penalties are subject to annual cost of living increases.[3]

Conduct of covered entity or business associate	**Penalty**
Did not know and, by exercising reasonable diligence, would not have known of the violation	$137 to $68,928 per violation; Up to $2,057,813 per identical violation per year
Violation due to reasonable cause and not willful neglect	$1,379 to $68,928 per violation; Up to $2,067,813 per identical violation per year
Violation due to willful neglect but the violation is corrected within 30 days after the covered entity knew or should have known of the violation	Mandatory fine of $13,785 to $68,928 per violation; Up to $2,067,813 per identical violation per year
Violation due to willful neglect and the violation was not corrected within 30 days after the covered entity knew or should have known of the violation	Mandatory fine of not less than $68,928 per violation; Up to $2,067,813 per identical violation per year

Significantly, a single act or omission may result in multiple violations. According to the US Department of Health and Human Services (HHS), the loss of a laptop containing records of 500 individuals may constitute 500 violations.[4] Similarly, if the violations were based on the failure to implement a required policy or safeguard, each day the

covered entity failed to have the required policy or safeguard in place constitutes a separate violation.[5] Not surprisingly, penalties can add up quickly. And the government is serious about the new penalties: the OCR has imposed millions of dollars in penalties or settlements since the mandatory penalties took effect.[6] State attorneys general may also sue for HIPAA violations and recover penalties of $25,000 per violation plus attorneys' fees.[7] Future regulations will allow affected individuals to recover a portion of any settlement or penalties arising from a HIPAA violation, thereby increasing individuals' incentive to report HIPAA violations.[8] And, while there is no private cause of action under HIPAA, affected patients or other individuals may use HIPAA to support a negligence *per se* or common law claim for damages.

The good news is that if the covered entity does *not* act with willful neglect, the OCR may waive or reduce the penalties, depending on the circumstances.[9] More importantly, if the covered entity or business associate does not act with willful neglect *and* corrects the violation within 30 days, the OCR may not impose any penalty; timely correction is an affirmative defense.[10]

2. HIPAA Violations May Be a Crime. Federal law prohibits any individual from improperly obtaining or disclosing protected health information (PHI) from a covered entity without authorization; violations may result in the following criminal penalties:[11]

Prohibited Conduct	**Penalty**
Knowingly obtaining or disclosing PHI without authorization.	Up to $50,000 fine and one year in prison
If done under false pretenses.	Up to $100,000 fine and five years in prison
If done with intent to sell, transfer, or use the PHI for commercial advantage, personal gain, or malicious harm.	Up to $250,000 fine and ten years in prison

Physicians, hospital staff members, and others have been prosecuted for improperly accessing, using, or disclosing PHI. Importantly, the criminal penalties apply whether or not the defendant is a covered entity or business associate under HIPAA and extend to employees, ex-employees, and others who may not be directly covered by HIPAA's civil penalties.

3. Covered Entities Must Self-Report HIPAA Breaches. The risk of penalties is compounded by the fact that covered entities must self-report HIPAA breaches of unsecured PHI to the affected individual, HHS, and, in certain cases, to the media.[12] Under the current standards, the unauthorized access, use, or disclosure of PHI in violation of the HIPAA

privacy rule is presumed to be reportable unless the covered entity or business associate can demonstrate a low probability that the data has been compromised through an assessment of specified risk factors.[13] Reporting a HIPAA violation is bad enough given the costs of notice, responding to government investigations, and potential penalties, but the consequences for failure to report a known breach are likely worse: if discovered, such a failure would likely constitute willful neglect, thereby subjecting the covered entity or business associate to the mandatory civil penalties.[14]

4. Potential for a Private Cause of Action. HIPAA does not expressly create a private cause of action for injured individuals, but plaintiffs may attempt to use HIPAA to establish the standard of care owed in a negligence claim. In addition, individuals may also sue under common law tort theories such as invasion of privacy, negligent infliction of emotional distress, or public disclosure of private facts. Even if the covered entity ultimately prevails, the entity may face the costs of the suit.

5. Other Federal and State Laws. Data privacy is a hot topic at both the state and federal level. A growing number of states have enacted their own data privacy laws that impose significant penalties for violations. In addition, the Federal Trade Commission (FTC) now actively pursues claims against entities who violate privacy standards or policies under the Section 5 of the Federal Trade Commission Act (FTCA).[15] Compliance with HIPAA standards will go a long way toward avoiding liability under various state and federal laws.

Given the risk of civil and criminal penalties, relatively low breach notification standards, and expanded enforcement, it is more important than ever for covered entities to comply or, at the very least, document good faith efforts to comply, to avoid a charge of willful neglect, mandatory penalties, and civil lawsuits. The following are key compliance actions that covered entities should take:

1. Assign HIPAA responsibility. Covered entities must designate persons to serve as their HIPAA privacy and security officers and document the designation in writing.[16] The privacy and security officers are responsible for ensuring HIPAA compliance. To that end, they should be thoroughly familiar with the requirements of the HIPAA Privacy,[17] Security,[18] and Breach Notification Rules.[19] The OCR maintains a very helpful website to assist covered entities in complying with the rules, http://www.hhs.gov/ocr/privacy/.

2. Know the use and disclosure rules. The basic privacy rules are relatively simple: covered entities may not use, access, or disclose PHI without the individual's valid, HIPAA-compliant authorization unless the use or disclosure fits within a HIPAA exception.[20] Unless they have agreed otherwise, covered entities may use or disclose PHI for purposes of treatment, payment, or certain healthcare operations without the individual's consent.[21] In addition, covered entities may use or disclose PHI for certain purposes so long as the individual has not objected, including use of certain PHI for facility directories or disclosure of PHI to family members or others involved in the individual's care or payment for

their care so long as the provider believes the disclosure is in the individual's best interests.[22] HIPAA contains numerous exceptions that allow disclosures of PHI to the extent another law requires disclosures or for certain public safety and government functions, including reporting of abuse and neglect; responding to government investigations; or disclosures to avoid a serious and imminent threat to the individual.[23] Even though HIPAA would allow a disclosure, the covered entity generally cannot disclose more than is minimally necessary for the intended purpose.[24] Covered entities generally must take reasonable steps to verify the identity of the person to whom the disclosure may be made.[25] The OCR has published a helpful summary of the Privacy Rule at https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

3. Know individuals' rights. HIPAA grants individuals certain rights concerning their PHI. Among others, individuals generally have a right to request limitations on otherwise permissible disclosures for treatment, payment, and healthcare operations;[26] request confidential communications at alternative locations or by alternative means;[27] access or obtain copies of their PHI, including e-PHI;[28] request amendments to their PHI;[29] and obtain an accounting of impermissible and certain other disclosures of PHI.[30] The OCR is actively enforcing patient rights, especially individuals' right to access their information.[31] The OCR's guidance on *Individuals' Right under HIPAA to Access their Health Information* is a must read for covered entities.[32]

4. Implement and maintain written policies. HIPAA requires covered entities to develop and maintain written policies that implement the Privacy, Security, and Breach Notification Rule requirements.[33] According to HHS, maintaining the required written policies is a significant factor in avoiding penalties imposed for "willful neglect."[34] Rite Aid paid $1,000,000 to settle HIPAA violations based in part on its failure to maintain required HIPAA policies.[35] A list of required and recommended privacy and breach notification polices is available at https://www.hollandhart.com/pdf/hipaa-privacy-checklist-hh.pdf; a list of required security policies is available at https://www.hollandhart.com/pdf/hipaa_checklist.pdf. Covered entities should periodically review and, as necessary, update their policies and practices to ensure ongoing compliance with HIPAA rules.

5. Develop compliant forms. HIPAA requires that certain documents used by covered entities satisfy regulatory requirements as described below. Covered entities should ensure that their HIPAA forms comply, although the OCR has suggested that technical non-compliance would likely not constitute willful neglect.[36]

a. **Authorizations.** HIPAA authorizations to use or disclose PHI must contain certain elements and required statements to be valid.[37] A checklist for authorizations is available at https://www.hollandhart.com/valid-hipaa-authorizations-a-checklist.

b. **Notice of privacy practices.** Covered entities must provide individuals with a notice of privacy practices (NPP) that

describes how the entity will use the individual's PHI and contains certain required statements.[38] The OCR has published model NPPs on its website, http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html, although most covered entities would likely prefer to use their own forms. A checklist for current NPP requirements is available at https://www.hollandhart.com/checklist-for-hipaa-notice-of-privacy-practices. Note, however, that NPP requirements are in a state of flux: covered entities must modify their NPPs by February 16, 2026, to comply with HHS's new rules concerning reproductive rights[39] and substance use disorder (SUD) information.[40]

c. **Other forms.** Although not required, covered entities may develop other forms to ensure compliance with individual rights, such as individual requests to access PHI, amend records, or obtain an accounting of disclosures.

6. Execute appropriate business associate agreements. Although HIPAA applies directly to business associates, HIPAA still requires covered entities to execute "business associate agreements" with their business associates before disclosing PHI to the business associate.[41] Business associates are generally those outside entities who create, receive, maintain, or transmit PHI on behalf of the covered entity.[42] "Business associates" include data storage companies and entities that provide data transmission services if they require routine access to PHI, and subcontractors of business associates.[43] If they have not done so recently, covered entities should immediately identify their business associates and ensure appropriate agreements are executed with them. A checklist for business associate agreements is available at https://www.hollandhart.com/business-associate-agreements-requirements-and-suggestions.

Breach of the business associate agreement exposes the business associate to contract claims by the covered entity in addition to HIPAA penalties. Covered entities are generally not liable for the actions of their business associates unless the covered entity knows of a pattern of activity or practice of the business associate that constitutes a material violation of the business associate's obligation and fails to act to cure the breach or end the violation,[44] or the business associate is acting as the agent of the covered entity.[45] To avoid liability, covered entities should ensure that business associates are acting as independent contractors, not agents of the covered entity.[46] For more suggestions to minimize liability for business associate conduct, see https://www.hollandhart.com/webfiles/HollandHart_Minimizing-Liability-for-Business-Associate-Misconduct.pdf.

7. Perform and document a risk analysis. The HIPAA Security Rule applies to PHI maintained in electronic form, *e.g.*, data on computers, mobile devices, USBs, *etc.*[47] Covered entities must periodically conduct and document a risk analysis of their computer and other information systems to identify potential security risks and respond accordingly.[48] HHS has updated its on-line risk assessment tool that covered entities may use

to perform their analysis; it is available at https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool. HHS has published additional guidance for the risk analysis, *e.g.*, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf. Covered entities should periodically review and update their risk analysis. A Massachusetts dermatology practice agreed to pay $150,000 for, among other things, failing to conduct an adequate risk assessment of its systems, including the use of USBs.[49]

8. Implement required safeguards. HHS recognizes that individual privacy cannot be absolutely protected; accordingly, HIPAA does not impose liability for "incidental disclosures" so long as the covered entity implemented reasonable administrative, technical, and physical safeguards designed to protect against improper disclosures.[50] The Security Rule contains detailed regulations specifying safeguards that must be implemented to protect e-PHI.[51] A checklist of required security safeguards is available at https://www.hollandhart.com/pdf/hipaa_checklist.pdf. The Privacy Rule is less specific; it simply requires that covered entities implement reasonable safeguards.[52] The reasonableness of the safeguards depends on the circumstances, but may include, *e.g.*, not leaving PHI where it may be lost or improperly accessed; checking e-mail addresses and fax numbers before sending messages; using fax cover sheets; *etc.* Covered entities should periodically evaluate its safeguards given changes in its practices, resources, and risks.

9. Train workforce. Having the required safeguards, policies, and forms is important, but covered entities and business associates must also train their workforce members to comply with their policies and document such training.[53] HIPAA requires that new employees receive training within a reasonable period of time after hire, and as needed thereafter.[54] According to HHS commentary, covered entities may avoid HIPAA penalties based on the misconduct of a rogue employee so long as the covered entity implemented appropriate policies and adequately trained the employee.[55]

10. Respond immediately to any violation or breach. This is critical for several reasons. First, HIPAA requires covered entities and business associates to investigate any privacy complaints, mitigate any breach, and impose appropriate sanctions against any agent who violates HIPAA.[56] It may also require covered entities to terminate an agreement with a business associate due to the business associate's noncompliance.[57] Second, prompt action may minimize or negate the risk that the data has been compromised, thereby allowing the covered entity or business associate to avoid self-reporting breaches to the individual or HHS.[58] Third, a covered entity or business associate can avoid HIPAA penalties altogether if it does not act with willful neglect and corrects the violation within 30 days.[59]

11. Timely report breaches. If a reportable breach of unsecured PHI occurs, covered entities must notify the individual within 60 days.[60] If the breach involves less than 500 persons, the covered entity must notify HHS by filing an electronic report no later than 60 days after the end of the

calendar year.[61] If the breach involves 500 or more persons, the covered entity must file the electronic report when it notifies the individual.[62] If the breach involves more than 500 persons in a state, the covered entity must notify local media.[63] The written notice to the individual must satisfy regulatory requirements concerning the manner and content of the notice.[64] For more information on identifying and responding to breaches, see https://www.hollandhart.com/responding-to-hipaa-breaches and https://www.hollandhart.com/hipaa-breach-notification-when-and-how-to-self-report.

12. Document actions. Documenting proper actions will help covered entities defend against HIPAA claims. Covered entities and business associates are required to maintain documentation required by HIPAA for six years from the date that the document was last in effect.[65]

13. Beware more stringent laws. In evaluating their compliance, covered entities must also consider other federal or state privacy laws. To the extent a state or other federal law is more stringent than HIPAA, covered entities should comply with the more restrictive law, including conditions of participation or licensing regulations that may apply to certain facilities.[66] In general, a law is more stringent than HIPAA if it offers greater privacy protection to individuals, or grants individuals greater rights regarding their PHI.[67]

14. Watch for Changes. As discussed, patient privacy is evolving at the state and federal level. In addition to the new reproductive rights and SUD information rules, additional proposed HIPAA changes are pending.[68] Covered entities must monitor and implement the changes to ensure ongoing compliance.

CONCLUSION.

Covered entities must comply with HIPAA or face draconian penalties. As many businesses have recently learned, even seemingly minor or isolated security lapses may result in major fines and business costs. Fortunately, however, covered entities may avoid mandatory fines and minimize their HIPAA exposure by taking and documenting the steps outlined above. Covered entities may use this outline to evaluate and, where needed, upgrade their overall HIPAA compliance.

[1] 45 CFR part 164.

[2] 45 CFR § 160.103, definition of “covered entity.”

[3] 45 CFR §§ 102.3 and 160.404.

[4] *See* HHS Request for Information re Civil Monetary Penalty (CMP) and Settlement Sharing at 87 FR 19833 (4/6/23).

[5] 45 CFR §160.406; 78 F.R. 5584 (1/25/13).

[6] The OCR's website contains data summarizing HIPAA enforcement activities, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html.

[7] 42 USC § 1320d-5(d); *see also* OCR training for state attorneys general at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/index.html.

[8] *See* 78 FR 5568 (1/25/13).

[9] 45 CFR § 160.308(a)(2) and 160.408.

[10] 45 CFR § 160.410.

[11] 42 USC § 1320d-6.

[12] 45 CFR § 164.400 *et seq.*

[13] 45 CFR § 164.402; 78 FR 5641 (1/25/13).

[14] 75 FR 40879 (7/14/10).

[15] *See, e.g.*, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement.

[16] 45 CFR §§ 164.308(a)(2) and 164.530(a).

[17] 45 CFR part 164, subpart E (§§ 164.500-164.534).

[18] 45 CFR part 164, subpart C (§§ 164.302-164.318).

[19] 45 CFR §164.502, Subpart D (§§ 164.400-414).

[20] 45 CFR §164.502

[21] 45 CFR §§164.506 and 164.522(a).

[22] *See* 45 CFR § 164.510.

[23] 45 CFR § 164.512.

[24] 45 CFR §§ 164.502(b) and 164.514(d).

[25] 45 CFR § 164.514(h).

[26] 45 CFR § 164.522(a).

[27] 45 CFR § 164.522(b).

[28] 45 CFR § 164.524.

[29] 45 CFR § 164.526.

[30] 45 CFR § 164.528.

[31] *See, e.g.*, https://www.hhs.gov/about/news/2024/04/01/hhs-office-civil-rights-imposes-civil-monetary-penalty-new-jersey-nursing-facility-failing-provide-timely-access-patient-records.html.

[32] https://www.hhs.gov/hipaa/for-

professionals/privacy/guidance/access/index.html.

[33] 45 CFR §§ 164.316(a), 164.404(a), and 164.530(f).

[34] *See* 75 FR 48078-79.

[35] *See* Press Release at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/rite-aid/index.html.

[36] 75 FR 40878 (7/14/10)

[37] 45 CFR § 164.508(c).

[38] 45 CFR § 164.520.

[39] 89 FR 32976 (4/26/24).

[40] 89 FR 12472 (2/16/24).

[41] 45 CFR §§ 164.308(b) and 164.502(e).

[42] 45 CFR § 160.103.

[43] 45 CFR § 160.103.

[44] 45 CFR § 164.504(e)(1).

[45] 45 CFR § 160.402(c).

[46] 78 FR 5581.

[47] 45 CFR § 164.103.

[48] 45 CFR § 164.308(a)(1).

[49] *See* Press Release at http://www.hhs.gov/news/press/2013pres/12/20131226a.html.

[50] 45 CFR § 164.502(a)(1); *see* Guidance at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/incidentalusesanddisclosures.html.

[51] 45 CFR §§ 164.308 to 164.316 and Appendix A to 45 CFR part 164, subpart C.

[52] 45 CFR § 164.530(c).

[53] 45 CFR § 164.530(b); *see also* 45 CFR §§ 164.308(a)(5) and 164.414(a).

[54] 45 CFR § 164.530(b).

[55] 75 FR 40879.

[56] 45 CFR § 164.530(d)-(f).

[57] 45 CFR §§164.314(a)(2) and 164.504(e)(2).

[58] 45 CFR § 164.402.

[59] 45 CFR § 160.410.

[60] 45 CFR § 164.404.

[61] 45 CFR § 164.408(c).

[62] 45 CFR § 164.408(b).

[63] 45 CFR § 164.406.

[64] 45 CFR § 164.404(c)-(d).

[65] 45 CFR §§ 164.316(b), 164.414(a), and 164.530(j).

[66] 45 CFR § 160.203.

[67] 45 CFR § 160.202.

[68] 86 FR 6446 (1/21/21).
