Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

Complying With HIPAA: A Checklist for Business Associates

Publication — 10/26/2015

The HIPAA Privacy, Security, and Breach Notification Rules now apply to both covered entities (*e.g.*, healthcare providers and health plans) and their business associates. A "business associate" is generally a person or entity who "creates, receives, maintains, or transmits" protected health information (PHI) in the course of performing services on behalf of the covered entity (*e.g.*, consultants; management, billing, coding, transcription or marketing companies; information technology contractors; data storage or document destruction companies; data transmission companies or vendors who routinely access PHI; third party administrators; personal health record vendors; lawyers; accountants; and malpractice insurers).[1] With very limited exceptions, a subcontractor or other entity that creates, receives, maintains, or transmits PHI on behalf of a business associate is also a business associate.[2] To determine if you are a business associate, see the attached Business Associate Decision Tree.

Business associates must comply with HIPAA for the following reasons:

1. Civil Penalties Are Mandatory for Willful Neglect. The Office for Civil Rights ("OCR") is required to impose HIPAA penalties if the business associate acted with willful neglect, *i.e.*, with "conscious, intentional failure or reckless indifference to the obligation to comply" with HIPAA requirements.[3] The following chart summarizes the tiered penalty structure:[4]

Conduct of covered entity or business associate	**Penalty**
Did not know and, by exercising reasonable diligence, would not have known of the violation	$100 to $50,000 per violation; Up to $1,500,000 per identical violation per year
Violation due to reasonable cause and not willful neglect	$1,000 to $50,000 per violation; Up to $1,500,000 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 $10,000 to $50,000 per violation; Up to $1,500,000 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	Mandatory fine of not less than $50,000 per violation; Up to $1,500,000 per identical

have known of the violation	violation per year

A single action may result in multiple violations. According to HHS, the loss of a laptop containing records of 500 individuals may constitute 500 violations.[5] Similarly, if the violation 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.[6] 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.[7] State attorneys general may also sue for HIPAA violations and recover penalties of $25,000 per violation plus attorneys' fees.[8] 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.[9]

The good news is that if the business associate does **not** act with willful neglect, the OCR may waive or reduce the penalties, depending on the circumstances.[10] More importantly, if the 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.[11] Whether business associates implemented required policies and safeguards is an important consideration in determining whether they acted with willful neglect.[12]

2. HIPAA Violations May Be A Crime. Federal law prohibits any individual from improperly obtaining or disclosing PHI from a covered entity without authorization; violations may result in the following criminal penalties:[13]

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.

3. Business Associates Must Self-Report HIPAA Breaches. The risk of penalties is compounded by the fact that business associates must self-report HIPAA breaches of unsecured PHI to covered entities,[14] and

covered entities must then report the breach to affected individual(s), HHS, and, in certain cases, to the media.[15] The Omnibus Rule modified the Breach Notification Rule to eliminate the former harm analysis; now a breach of PHI 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.[16] 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.[17]

Given the increased penalties, lowered breach notification standards, and expanded enforcement, it is more important than ever for business associates 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 business associates should take.

1. Determine whether business associate rules apply. Out of ignorance or an abundance of caution, covered entities may ask some entities to sign business associate agreements even though the entity is not a "business associate" as defined by HIPAA. Entities should avoid assuming business associate liabilities or entering business associate agreements if they are not truly business associates. Significantly, the following are not business associates: (i) entities that do not create, maintain, use, or disclose PHI in performing services on behalf of the covered entity; (ii) members of the covered entity's workforce; (iii) other healthcare providers when providing treatment; (iv) members of an organized healthcare arrangement; (v) entities who use PHI while performing services on their own behalf, not on behalf of the covered entity; and (vi) entities that are mere conduits of the PHI.[18] For more information on avoiding business associate agreements, see this link.

2. Execute and comply with valid business associate agreements. Entities that are business associates must execute and perform according to written business associate agreements that essentially require the business associate to maintain the privacy of PHI; limit the business associate's use or disclosure of PHI to those purposes authorized by the covered entity; and assist covered entities in responding to individual requests concerning their PHI.[19] The OCR has published sample business associate agreement language on its website: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

Covered entities may sometimes add terms or impose obligations in business associate agreements that are not required by HIPAA. Business associates should review business associate agreements carefully to ensure they do not unwittingly assume unintended obligations, such as indemnification provisions or requirements to carry insurance. Conversely, business associates may want to add terms to limit their liability, such as liability caps, mutual indemnification, *etc.* A checklist for business

associate agreements and suggested terms is available at this link.

3. Execute valid subcontractor agreements. If the business associate uses subcontractors or other entities to provide any services for the covered entity involving PHI, the business associate must execute business associate agreements with the subcontractors, which agreements must contain terms required by the regulations.[20] The subcontractor becomes a business associate subject to HIPAA.[21] The subcontractor agreement cannot authorize the subcontractor to do anything that the business associate could not do under the original business associate agreement with the covered entity.[22] Thus, business associate obligations are passed downstream to subcontractors.[23] Business associates are not liable for the business associate's HIPAA violations unless the business associate was aware of a pattern or practice of violations and failed to act,[24] or the subcontractor is the agent of the business associate.[25] To be safe, business associates should confirm that their subcontractors are independent contractors.

4. Comply with privacy rules. Most of the Privacy Rule provisions do not apply directly to business associates,[26] but because business associates cannot use or disclose PHI in a manner contrary to the limits placed on covered entities,[27] business associates will likely need to implement many of the same policies and safeguards that the Privacy Rule mandates for covered entities, including rules governing uses and disclosure of PHI and individual rights concerning their PHI. Those are typically outlined in the business associate's agreement with the covered entity.[28] Business associates should generally be aware of the Privacy Rule requirements along with any additional limitations or restrictions that the covered entity may have imposed on itself through its notice of privacy practices or agreements with individuals.

The basic privacy rules are relatively simple: covered entities and their business associates may not use, access, or disclose PHI without the individual's valid, HIPAA-compliant authorization, unless the use or disclosure fits within an exception.[29] Unless they have agreed otherwise, covered entities and business associates may use or disclose PHI for purposes of treatment, payment or certain health care operations without the individual's consent.[30] 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; however, before making disclosures for such purposes, the business associate should consult with the covered entity.[31] Even where disclosure is allowed, business associates must generally limit their requests for or use or disclosure of PHI to the minimum necessary for the intended purpose.[32] The OCR has published a helpful summary of the Privacy Rule: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf. (Please note that the summary has not been updated to reflect changes in the Omnibus Rule.)

5. Perform a Security Rule risk analysis. Unlike the Privacy Rule, business associates are directly obligated to comply with the Security

Rule.[33] Business associates must conduct and document a risk analysis of their computer and other information systems to identify potential security risks and respond accordingly.[34] HHS has developed and made available a risk assessment tool for covered entities and business associates: https://www.healthit.gov/providers-professionals/security-risk-assessment-tool. In addition, the OCR has published guidance for the risk analysis at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf. Business associates should periodically review and update their risk analysis. A Massachusetts dermatology practice recently agreed to pay $150,000 for, among other things, failing to conduct an adequate risk assessment of its systems, including the use of USBs.

6. Implement Security Rule safeguards. Like covered entities, business associates must implement the specific administrative, technical and physical safeguards required by the Security Rule.[35] A checklist of the required security rule policies is available here.

7. Adopt written Security Rule policies. As with covered entities, business associates must adopt and maintain the written policies required by the Security Rule.[36] A checklist of required polices is available at this link. According to HHS, maintaining the required written policies is a significant factor in avoiding penalties imposed for "willful neglect." Rite Aid paid $1,000,000 to settle HIPAA violations based in part on its failure to maintain required HIPAA policies.

8. Train personnel. Unlike covered entities, the Privacy and Breach Notification Rules do not affirmatively require business associates to train their workforce members, but the Security Rule does.[37] As a practical matter, business associates will need to train their workforce concerning the HIPAA rules to comply with the business associate agreement and HIPAA regulations. Documenting such training may prevent HIPAA violations and/or avoid allegations of willful neglect if a violation occurs.

9. Respond immediately to any violation or breach. The Privacy Rule does not impose any specific requirement on business associates to mitigate violations, but many business associate agreements do. Even if not required by rule or contract, business associates will want to respond immediately to any real or potential violation to mitigate any unauthorized access to PHI and reduce the potential for HIPAA penalties. 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. In addition, as discussed above, a business associate can avoid HIPAA penalties altogether if it does not act with willful neglect and corrects the violation within 30 days.[38]

10. Timely report security incidents and breaches. Business associates must notify the covered entity of certain threats to PHI. First, business associates must report breaches of unsecured protected PHI to the covered entity so the covered entity may report the breach to the individual and HHS.[39] Second, the business associate must report uses or disclosures that violate the business associate agreement with the covered entity, which would presumably include uses or disclosures in violation of HIPAA even if not reportable under the breach notification rules.[40] Third,

business associates must report “security incidents,” which is defined to include the “attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or interference with system operations in a PHI system.”[41]

11. Maintain Required Documentation. Business associates must maintain the documents required by the Security Rule for six years from the document's last effective date.[42] Although not required, documenting other acts in furtherance of compliance may help negate any allegation of willful neglect.

12. Beware more stringent laws. In evaluating their compliance, business associates must also consider other federal or state privacy laws. To the extent a state or other federal law is more stringent than HIPAA, business associates should comply with the more restrictive law.[43] 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.[44]

CONCLUSION.
Like covered entities, business associates must now 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, business associates may avoid mandatory fines and minimize their HIPAA exposure by taking and documenting the steps outlined above. Business associates may use this outline to evaluate and, where needed, upgrade their overall compliance.

For questions regarding this update, please contact:
Kim C. Stanger
Holland & Hart, 800 W Main Street, Suite 1750, Boise, ID 83702
email: kcstanger@hollandhart.com, phone: 208-383-3913

---

[1]45 CFR 160.103, definition of “business associate.”
[2]*Id.*; 78 FR 5572.
[3]45 CFR § 160.401 and 164.404.
[4]45 CFR § 160.404.
[5]*See* 78 FR 5584 (1/25/13).
[6] 45 CFR §160.406; 78 F.R. 5584 (1/25/13).
[7]The OCR's website contains data summarizing HIPAA enforcement activities, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html.
[8]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.
[9]*See* 78 FR 5568 (1/25/13).
[10]45 CFR § 160.308(a)(2) and 160.408.
[11]45 CFR § 160.410.
[12]*See* Press Releases of various cases reported at http://www.hhs.gov/ocr/office/index.html.
[13]42 USC § 1320d-6.
[14]42 CFR § 164.410.
[15]45 CFR § 164.400 *et seq*.
[16]45 CFR § 164.402; 78 FR 5641 (1/25/13).
[17]75 FR 40879 (7/14/10).
[18]45 CFR § 160.103; 78 FR 5571 (1/25/13).
[19]45 CFR 164.504(e).
[20]45 CFR §§ 164.314(a)(2) and 164.504(e)(1).
[21]45 CFR 160.103.
[22]45 CFR §§164.314(a)(2) and 164.504(e)(5).
[23]78 FR 5573 (1/25/13).
[24]45 CFR § 164.504(e)(1).
[25]45 CFR § 160.402(c).
[26]78 FR 5591 (1/25/13).
[27]45 CFR § 164.504(e)(2); 78 FR 5591 (1/25/13).
[28]*See* 45 CFR § 164.502(e).
[29]45 § CFR 164.502.
[30]45 § CFR 164.506.
[31]45 § CFR 164.510 and .512.
[32]45 CFR § 164.502(b)(1).
[33]45 CFR § 164.314(a)(2).
[34]45 CFR § 164.308(a)(1).
[35]45 CFR §§ 164.306(a), 164.308(a), 164.310, and 164.312.
[36]45 CFR § 164.316.
[37]45 CFR §§ 164.308(a)(5)
[38]45 CFR §§ 160.410.
[39]45 CFR § 164.410.
[40]45 CFR § 164.504(e)(2).
[41]45 CFR § 164.304.
[42]45 CFR § 164.316(a)(2).
[43]45 CFR § 160.203.
[44]45 CFR § 160.202.