HOLLAND&HART LLP

HIPAA UPDATE 2014:
WHY AND HOW YOU MUST COMPLY[1]

In January 2013, the Department of Health and Human Services ("HHS") issued its long-awaited Omnibus Rule[2] implementing regulations required by the HITECH Act[3] and significantly expanding HIPAA[4] requirements and penalties associated with the misuse or improper disclosure of protected health information ("PHI"). Among other things, the Omnibus Rule extends HIPAA to business associates[5] of covered entities and raised the stakes on regulatory compliance. This memorandum outlines key actions that covered entities and business associates should take to help ensure their compliance and avoid HIPAA penalties.

WHY YOU NEED TO COMPLY.

1. **Civil Penalties Are Mandatory for Willful Neglect.** HITECH increased the penalties for HIPAA violations 500 times their prior limits. The Office for Civil Rights ("OCR") is required to impose HIPAA penalties if the covered entity or business associate acted with willful neglect, *i.e.*, with "conscious, intentional failure or reckless indifference to the obligation to comply" with HIPAA requirements.[6] The following chart summarizes the tiered penalty structure[7]:

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 have known of the violation	Mandatory fine of not less than $50,000 per violation; Up to $1,500,000 per identical 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.[8] Similarly, if the violation were based on the failure to implement a required policy or safeguard, each day the entity failed to have the required policy or safeguard in place constitutes a separate violation.[9] 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.[10] State attorneys general may also sue for HIPAA violations and recover penalties of $25,000 per violation plus attorneys' fees.[11] 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.[12]

The good news is that if the covered entity or business associate does not act with willful neglect, the OCR may waive or reduce the penalties, depending on the circumstances.[13] 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.[14] Whether covered entities or business associates implemented required policies and safeguards is an important consideration in determining whether they acted with willful neglect.[15]

Copyright © 2014, Holland & Hart LLP

Kim C. Stanger
208-383-3913
kcstanger@hollandhart.com
www.hollandhart.com
www.hhhealthlawblog.com

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[16]:

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. **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.[17] Business associates must report such breaches to the covered entity so the covered entity may give the required notice.[18] 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.[19] 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.[20]

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

WHAT COVERED ENTITIES SHOULD DO TO COMPLY.

Covered entities are health plans (including employee group plans that have 50 or more participants or that are administered by a third party; health care clearinghouses; and health care providers who engage in certain electronic transactions.[21] 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.[22] 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[23], Security[24], and Breach Notification Rules.[25] The OCR maintains a very helpful website to assist covered entities and business associates 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 an exception.[26] Unless they have agreed otherwise, covered entities may use or disclose PHI for purposes of treatment, payment or certain health care operations without the individual's consent.[27] In addition, covered entities may use or disclose PHI for certain purposes so long as the individual has not objected,

Copyright © 2014, Holland & Hart LLP

Kim C. Stanger
208-383-3913
kcstanger@hollandhart.com
www.hollandhart.com
www.hhhealthlawblog.com

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 such disclosure is in the individuals' best interests.[28] 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.[29] Even though HIPAA would allow a disclosure, the covered entity and business associate generally cannot disclose more than is minimally necessary for the intended purpose.[30] Covered entities and business associates generally must take reasonable steps to verify the identity of the person to whom the disclosure may be made.[31] The OCR has published a helpful summary of the Privacy Rule at http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf, although the summary has not been updated to reflect changes in the Omnibus Rule.

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[32]; request confidential communications at alternative locations or by alternative means[33]; access or obtain copies of their PHI, including e-PHI[34]; request amendments to their PHI[35]; and obtain an accounting of impermissible and certain other disclosures of PHI.[36] Covered entities and business associates must know and allow individuals to exercise their rights. One health system was fined $4.3 million for, among other things, failing to timely respond to individual requests to access their PHI.[37]

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.[38] According to HHS, maintaining the required written policies is a significant factor in avoiding penalties imposed for "willful neglect."[39] Rite Aid paid $1,000,000 to settle HIPAA violations based in part on its failure to maintain required HIPAA policies.[40] For a list of required and recommended privacy and breach notification polices see the attached Appendix 1 – HIPAA Privacy Checklist; for a list of required security policies see the attached Appendix 2 – HIPAA Security Checklist. If they have not done so, covered entities should update their privacy and breach notification policies to comply with the new Omnibus Rule provisions described below.

a. **Deceased persons**. Covered entities may now disclose PHI to family members or others who were involved in the decedent's health care or payment for their care prior to the decedent's death so long as the disclosure is relevant to the person's involvement and is not inconsistent with the decedent's prior expressed preferences.[41]

b. **Individual access to e-PHI**. If an individual requests an electronic copy of their PHI, covered entities must generally produce it in the form requested if readily producible.[42] If the individual directs the covered entity in writing to transmit a copy of their e-PHI to another individual, the covered entity must generally comply.[43]

c. **Time for responding to request to access**. Covered entities must generally respond to an individual's request to access their PHI within 30 days; the Omnibus Rule eliminated the provision that gave covered entities extra time to respond if records were maintained offsite.[44]

d. **Limits on disclosures to insurers**. Covered entities may not disclose PHI about an individual's episode of care to a health insurer if (i) the insurer seeks the PHI for treatment or payment purposes; (ii) the individual or someone on the individual's behalf paid for the care to which the PHI pertains; and (iii) the individual requests that the PHI be withheld from the insurer.[45] This new rule will require covered entities to develop new and problematic processes for flagging and isolating such data from health insurer requests; fortunately, however, the requirement is only triggered if the individual requests such limitations, which should rarely occur. HHS's commentary to the Omnibus Rule is particularly helpful in understanding the limits of this new requirement.[46]

Copyright © 2014, Holland & Hart LLP

Kim C. Stanger
208-383-3913
kcstanger@hollandhart.com
www.hollandhart.com
www.hhhealthlawblog.com

e. **School immunizations**. Covered entities may now disclose PHI about immunizations to a school if (i) state law requires such PHI for school enrollment; and (ii) the individual or their personal representative consents to the disclosure. The consent may be oral.[47]

f. **Sale of PHI**. Covered entities must obtain written authorization to sell an individual's PHI, and the authorization must disclose that the sale will result in remuneration to the covered entity.[48]

g. **Marketing**. Covered entities must obtain written authorization to use the individual's PHI for marketing purposes, including most non-face-to-face communications for treatment purposes if the covered entity receives financial remuneration to make the communication.[49] If remuneration is involved, the marketing authorization must disclose that fact.[50]

h. **Fundraising**. The Omnibus Rule allows covered entities to disclose more PHI to institutionally related foundations to assist with fundraising, but fundraising communications must explain how the recipient may opt out of receiving such communications and the opt out method may not be burdensome.[51]

i. **Research**. If the covered entity engages in research, it should review new standards applicable to research as described in 45 CFR § 164.508(b).

j. **Breach notification.** The Omnibus Rule modified the standard for reporting breaches of unsecured PHI. Under the new standard, the unauthorized acquisition, access, use or disclosure of PHI in violation of the Privacy Rule is presumed to be a reportable breach unless (i) the covered entity or business associate demonstrates there is a low probability that the PHI has been compromised based on a risk assessment of certain factors, or (ii) the breach fits within certain exceptions.[52] Covered entities must ensure that their policies incorporate and that they apply this new, arguably lower standard. Given the lower standard, covered entities and business associates may want to consider "securing" e-PHI by encryption to the extent possible to avoid reportable breaches.

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.[53] Appendix 1 includes a list of recommended forms.

a. **Authorizations.** HIPAA authorizations to use or disclose PHI must contain certain elements and required statements to be valid.[54] The Omnibus Rule added a requirement that the authorization disclose that the covered entity receives remuneration if the covered entity seeks the authorization to sell PHI.[55]

b. **Notice of privacy practices.** Covered entities must provide individuals with a notice of privacy practices that describes how the entity will use the individual's PHI and contains certain required statements.[56] In addition to the items required by the prior rules, the Omnibus Rule requires covered entities to update their notices to also include the following: (i) a description of the types of PHI that require an authorization, *i.e.*, psychotherapy notes, marketing, and sale of PHI; (ii) a statement that other uses or disclosures not described in the notice will require an authorization; (iii) a statement that the recipient of fundraising materials may opt out; (iv) a description of the individual's right to limit disclosures to insurers if the individual paid for the relevant care; and (v) a statement that the covered entity must notify the individual of a breach of unsecured PHI.[57] In addition to updating their own notices, covered entities relying on joint notices should ensure the joint notices have been updated.[58] The OCR has recently published model privacy notices on its website, http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html, although most covered entities would likely prefer to use their own forms.

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,

Copyright © 2014, Holland & Hart LLP

Kim C. Stanger
208-383-3913
kcstanger@hollandhart.com
www.hollandhart.com
www.hhhealthlawblog.com

amend records, or obtain an accounting of disclosures. Appendix 1 contains a list of recommended forms.

6. **Execute appropriate business associate agreements.** Although HIPAA now 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.[59] Business associates are generally those outside entities who create, receive, maintain, or transmit PHI on behalf of the covered entity.[60] The Omnibus Rule expanded the definition of "business associates" to include data storage companies, entities that provide data transmission services if they require routine access to PHI, and subcontractors of business associates.[61] If they have not done so recently, covered entities should immediately identify their business associates and ensure appropriate agreements are executed with them.

Business associate agreements must contain certain elements, including (i) a description of permissible uses or disclosures of PHI; (ii) requirements to help the covered entity respond to individual rights; and (iii) certain termination provisions.[62] In addition to previous requirements, the Omnibus Rule now requires the business associate to: (i) comply with the security rule[63]; (ii) execute business associate agreements with their subcontractors[64]; (iii) if the business associate carries out an obligation of a covered entity, comply with any HIPAA rule applicable to such obligation[65]; and (iv) report breaches of unsecured PHI to the covered entity.[66] Covered entities should ensure their business associate agreements contain the Omnibus Rule terms. Covered entities have until September 22, 2014 to modify business associate agreements if (i) the agreement they had in place on January 25, 2013 complied with the HIPAA rules as of that date, and (ii) the agreement does not expire or renew (other than through evergreen clauses) prior to September 22, 2014.[67]

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,[68] or the business associate is acting as the agent of the covered entity.[69] To avoid liability, covered entities should ensure that business associates are acting as independent contractors, not agents of the covered entity.[70]

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.*[71] Covered entities and business associates must conduct and document a risk analysis of their computer and other information systems to identify potential security risks and respond accordingly.[72] The OCR has published guidance for the risk analysis at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf. Covered entities and 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.[73]

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.[74] The Security Rule contains detailed regulations specifying safeguards that must be implemented to protect e-PHI.[75] Appendix 2 contains a checklist of required security safeguards. The Privacy Rule is less specific; it simply requires that covered entities implement reasonable safeguards.[76] 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.*

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 the policies and document such training.[77] HIPAA requires that new employees

Copyright © 2014, Holland & Hart LLP

Kim C. Stanger
208-383-3913
kcstanger@hollandhart.com
www.hollandhart.com
www.hhhealthlawblog.com

are trained within a reasonable period of time after hire, and as needed thereafter.[78] 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.[79] If they have not done so, covered entities should train staff and other workforce members concerning the new Omnibus Rule requirements as discussed above.

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.[80] It may also require covered entities to terminate an agreement with a business associate due to the business associate's noncompliance.[81] 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.[82] 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.[83]

11. **Timely report breaches.** If a reportable breach of unsecured PHI occurs, business associates must promptly report the breach to covered entities,[84] and covered entities must notify the individual within 60 days.[85] 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.[86] If the breach involves 500 or more persons, the covered entity must file the electronic report when it notifies the individual.[87] If the breach involves more than 500 persons in a state, the covered entity must notify local media.[88] The written notice to the individual must satisfy regulatory requirements concerning the manner and content of the notice.[89]

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.[90]

WHAT BUSINESS ASSOCIATES SHOULD DO TO COMPLY.

Effective September 23, 2013, the OCR may impose penalties directly against business associates of covered entities for failing to comply with HIPAA requirements. In addition, business associates may be liable to covered entities if they breach their business associate agreement. The following outline summarizes what business associates should do to minimize their potential liability under HIPAA.

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.[91]

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.[92] 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,

Copyright © 2014, Holland & Hart LLP

Kim C. Stanger
208-383-3913
kcstanger@hollandhart.com
www.hollandhart.com
www.hhhealthlawblog.com

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.*

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.[93] The subcontractor becomes a business associate subject to HIPAA.[94] 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.[95] Thus, business associate obligations are passed downstream to subcontractors.[96] As with covered entities, 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,[97] or the subcontractor is the agent of the business associate.[98] 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,[99] but because business associates cannot use or disclose PHI in a manner contrary to the limits placed on covered entities,[100] 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.[101] 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. Among other things, business associates must generally limit their requests for or use or disclosure of PHI to the minimum necessary for the intended purpose.[102]

5. **Perform a Security Rule risk analysis**. Unlike the Privacy Rule, business associates are directly obligated to comply with the Security Rule.[103] Thus, like covered entities, business associates must conduct and document an appropriate risk analysis as described above.[104]

6. **Implement Security Rule safeguards.** Also like covered entities, business associates must implement the specific administrative, technical and physical safeguards required by the Security Rule as described above.[105] Appendix 2 contains a list of Security Rule requirements.

7. **Adopt written Security Rule policies.** As with covered entities, business associates must adopt and maintain the written policies required by the Security Rule[106] as described in Appendix 2.

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.[107] 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. Remember: timely action to correct a violation within 30 days is a key to avoiding or reducing HIPAA penalties.[108]

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

Copyright © 2014, Holland & Hart LLP

Kim C. Stanger
208-383-3913
kcstanger@hollandhart.com
www.hollandhart.com
www.hhhealthlawblog.com

breach to the individual and HHS.[109] 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.[110] 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."[111]

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.[112] Although not required, documenting other acts in furtherance of compliance may help negate any allegation of willful neglect.

BEWARE MORE STRINGENT LAWS.

In evaluating their compliance, covered entities and 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, covered entities and business associates should comply with the more restrictive law, including conditions of participation or licensing regulations that may apply to certain facilities.[113] 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.[114]

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, however, covered entities and business associates may avoid mandatory fines and minimize their HIPAA exposure by taking and documenting the steps outlined above. Accordingly, in addition to updating their policies and practices to comply with new Omnibus Rule requirements discussed above, covered entities should use this outline to evaluate and, where needed, upgrade their overall HIPAA compliance.

[1] This outline provides a summary of some of the relevant compliance issues and requirements. It is provided for educational purposes only. Readers should review the applicable laws and regulations and consult their own counsel when responding to compliance concerns.
[2] 78 F.R. 5566 (1/25/13).
[3] Health Information Technology for Economic and Clinical Health Act of 2009.
[4] Health Insurance Portability and Accountability Act of 1996.
[5] Under HIPAA, "business associates" are generally defined as those entities outside of the covered entity's workforce who create, receive, maintain or transmit protected health information ("PHI") on behalf of a covered entity to perform a function regulated by HIPAA or certain other enumerated functions, including claims processing; data analysis; utilization review; quality assurance; individual safety activities; billing; benefit management; practice management; legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services; data transmission services if routine access to data is required; and subcontractors of business associates. 45 CFR § 160.103.
[6] 45 CFR § 160.401 and 164.404.
[7] 45 CFR § 160.404.
[8] *See* 78 FR 5584 (1/25/13).
[9] 45 CFR §160.406; 78 F.R. 5584 (1/25/13).
[10] The OCR's website contains data summarizing HIPAA enforcement activities, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html.
[11] 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.
[12] *See* 78 FR 5568 (1/25/13).
[13] 45 CFR § 160.308(a)(2) and 160.408.
[14] 45 CFR § 160.410.
[15] *See* Press Releases of various cases reported at http://www.hhs.gov/ocr/office/index.html.
[16] 42 USC § 1320d-6.
[17] 45 CFR § 164.400 *et seq.*
[18] 45 CFR § 164.410.
[19] 45 CFR § 164.402; 78 FR 5641 (1/25/13).
[20] 75 FR 40879 (7/14/10).
[21] 45 CFR § 160.103.
[22] 45 CFR §§ 164.308(a)(2) and 164.530(a).

Copyright © 2014, Holland & Hart LLP

Kim C. Stanger
208-383-3913
kcstanger@hollandhart.com
www.hollandhart.com
www.hhhealthlawblog.com

[23] 45 CFR part 164, subpart E (§§ 164.500-164.534).
[24] 45 CFR part 164, subpart C (§§ 164.302-164.318).
[25] 45 CFR §164.502, Subpart D (§§ 164.400-414).
[26] 45 CFR §164.502.
[27] 45 CFR §§164.506 and 164.522(a).
[28] *See* 45 CFR § 164.510.
[29] 45 CFR § 164.512.
[30] 45 CFR §§ 164.502(b) and 164.514(d).
[31] 45 CFR § 164.514(h).
[32] 45 CFR § 164.522(a).
[33] 45 CFR § 164.522(b).
[34] 45 CFR § 164.524.
[35] 45 CFR § 164.526.
[36] 45 CFR § 164.528.
[37] *See* Press Release at http://www.hhs.gov/news/press/2011pres/02/20110222a.html.
[38] 45 CFR §§ 164.316(a), 164.404(a), and 164.530(f).
[39] *See* 75 FR 48078-79.
[40] *See* Press Release at http://www.hhs.gov/news/press/2010pres/07/20100727a.html.
[41] 45 CFR § 164.510(b)(5).
[42] 45 CFR § 164.524(c)(2).
[43] 45 CFR § 164.524(c)(3).
[44] 45 CFR § 164.524.
[45] 45 CFR § 164.522(a)(1).
[46] 78 FR 5626-5630 (1/25/13).
[47] 45 CFR § 164.512(b)(1).
[48] 45 CFR §§ 164.502(a)(5) and 164.508(a)(4).
[49] 45 CFR §§ 164.501 and 164.508(c).
[50] 45 CFR § 154.508(c).
[51] 45 CFR § 164.512(f).
[52] 45 CFR § 164.402.
[53] 75 FR 40878 (7/14/10).
[54] 45 CFR § 164.508(c).
[55] 45 CFR § 164.508(a)(4).
[56] 45 CFR § 164.520.
[57] 45 CFR § 164.520(b)(1).
[58] *See* 45 CFR § 164.520(d).
[59] 45 CFR §§ 164.308(b) and 164.502(e).
[60] 45 CFR § 160.103.
[61] 45 CFR § 160.103.
[62] 45 CFR § 164.504(e).
[63] 45 CFR § 164.314(a)(2).
[64] 45 CFR §§ 164.314(a)(2).
[65] 45 CFR § 164.504(e)(2)(ii)(H).
[66] 45 CFR §§ 164.314(a)(2)(i)(C).
[67] 45 CFR § 164.532(e).
[68] 45 CFR § 164.504(e)(1).
[69] 45 CFR § 160.402(c).
[70] 78 FR 5581.
[71] 45 CFR § 164.103.
[72] 45 CFR § 164.308(a)(1).
[73] *See* Press Release at http://www.hhs.gov/news/press/2013pres/12/20131226a.html.
[74] 45 CFR § 164.502(a)(1); *see* Guidance at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/incidentalusesanddisclosures.html.
[75] 45 CFR §§ 164.308 to 164.316 and Appendix A to 45 CFR part 164, subpart C.
[76] 45 CFR § 164.530(c).
[77] 45 CFR § 164.530(b); *see also* 45 CFR §§ 164.308(a)(5) and 164.414(a).
[78] 45 CFR § 164.530(b).
[79] 75 FR 40879.
[80] 45 CFR § 164.530(d)-(f).
[81] 45 CFR §§164.314(a)(2) and 164.504(e)(2).
[82] 45 CFR § 164.402.
[83] 45 CFR § 160.410.
[84] 45 CFR § 164.410.
[85] 45 CFR § 164.404.
[86] 45 CFR § 164.408(c).
[87] 45 CFR § 164.408(b).
[88] 45 CFR § 164.406.
[89] 45 CFR § 164.404(c)-(d).
[90] 45 CFR §§ 164.316(b), 164.414(a), and 164.530(j).

Copyright © 2014, Holland & Hart LLP

Kim C. Stanger
208-383-3913
kcstanger@hollandhart.com
www.hollandhart.com
www.hhhealthlawblog.com

[91] 45 CFR § 160.103; 78 FR 5571 (1/25/13).
[92] 45 CFR 164.504(e).
[93] 45 CFR §§ 164.314(a)(2) and 164.504(e)(1).
[94] 45 CFR 160.103.
[95] 45 CFR §§164.314(a)(2) and 164.504(e)(5).
[96] 78 FR 5573 (1/25/13).
[97] 45 CFR § 164.504(e)(1).
[98] 45 CFR § 160.402(c).
[99] 78 FR 5591 (1/25/13).
[100] 45 CFR § 164.504(e)(2); 78 FR 5591 (1/25/13).
[101] *See* 45 CFR § 164.502(e).
[102] 45 CFR § 164.502(b)(1).
[103] 45 CFR § 164.314(a)(2).
[104] 45 CFR § 164.308(a)(1).
[105] 45 CFR §§ 164.306(a), 164.308(a), 164.310, and 164.312.
[106] 45 CFR § 164.316.
[107] 45 CFR §§ 164.308(a)(5).
[108] 45 CFR §§ 160.410.
[109] 45 CFR § 164.410.
[110] 45 CFR § 164.504(e)(2).
[111] 45 CFR § 164.304.
[112] 45 CFR § 164.316(a)(2).
[113] 45 CFR § 160.203.
[114] 45 CFR § 160.202.

Copyright © 2014, Holland & Hart LLP

Kim C. Stanger
208-383-3913
kcstanger@hollandhart.com
www.hollandhart.com
www.hhhealthlawblog.com