I. HIPAA Implications of Physician-Hospital Integration

As physicians and hospitals become increasing integrated, regulatory compliance is a key consideration. The manner in which the parties will protect the privacy and security of PHI, while appropriately accessing the PHI necessary to achieve the parties’ objectives, must be addressed.

1.1 Affiliated Covered Entities (ACEs): Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of the Privacy and Security Rule.¹

A. The covered entities must all be under common ownership or common control. Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policy of another entity. Common ownership exists if an entity or entities possess an ownership or equity interest of 5% or more in another entity.²

B. For example, a health system could own a hospital, medical groups and DME supplier and designate them as an ACE.

C. Note that each member of the ACE must be a covered entity. If the parent company of the operating companies/providers in a health system or other integrated delivery system is not covered entity, then it cannot be part of the ACE. However, it could enter into a business associate agreement with the ACE which outlines how it will use and disclose PHI on behalf of the ACE.

D. The designation of an ACE must be documented and maintained for 6 years from the date of its creation or the date when it was last in effect, whichever is later.³

i. No specifics are given regarding the documentation required.

ii. Health systems which form ACEs must develop process for maintaining current documentation of component members (for example, if an additional physician practice is acquired).

E. If the ACE combines the functions of a health plan, provider or clearinghouse, it must comply with all applicable standards.⁴

F. An ACE may adopt and implement one set of policies and procedures, a common training program, and a single Notice of Privacy Practices, have a common privacy officer and jointly enter into Business Associate Agreements.

¹ 45 C.F.R. § 164.105(b)(1).
² 45 C.F.R. § 164.105(b)(2)(A) and 164.103.
³ 45 C.F.R. § 164.105(b)(2)(i)(B) and (c).
⁴ 45 C.F.R. § 164.105(b)(2)(ii).
i. Health systems need to determine if a uniform set of policies, etc. will be practical and effective when combining different care settings and types of providers.

ii. Even without a formally designated ACE, providers with common ownership or other affiliation could have a business associate relationship with a common parent company/management entity to provide oversight of HIPAA policies and procedures, training, forms, etc.

G. Joint liability for ACE participants: A covered entity that is a member of an ACE is jointly and severally liable for a civil monetary penalty for a violation of the Privacy and Security Rule based on an act or omission of the ACE, unless it is established that another member of the ACE was responsible for the violation.5

i. Depending on manner of affiliation, ACE members may wish to document individual liability for violations despite shared administrative oversight of HIPAA programs.

ii. ACE members must also assess whether members should enter into agreements regarding indemnification, etc.

H. WellPoint, Inc. Resolution Agreement. On July 8, 2013, HHS entered into Resolution Agreement with WellPoint, Inc. related to health plans under its ownership or control that had been designated as an ACE. WellPoint notified HHS of a breach involving PHI of approximately 612,000 individuals. HHS investigated and found that WellPoint did not have adequate security safeguards in place. WellPoint paid $17M to settle the matter. Notably, WellPoint, Inc., the settling party, is not a covered entity.6 The investigation and resolution demonstrates how the activities of ACE participants may implicate others in the arrangement, including the party deemed to responsible for HIPAA compliance of the participants.

1.2 Organized Health Care Arrangements (OHCAs): The regulations for OHCAs permit certain providers that are not commonly controlled or owned but are clinically integrated to share PHI. For example, a hospital and its medical staff can designate themselves as an OHCA and use PHI for joint activities, including quality assurance and peer review.

A. HIPAA defines an OHCA as follows:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities:

   (i) Hold themselves out to the public as participating in a joint arrangement; and

---

5 45 CFR § 160.402 (b).
(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or performance, or operations; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

B. A covered entity that participates in an OHCA may disclose PHI about an individual to other participants for any health care operations activities of the OHCA.7

C. The definition of business associate specifically excludes a covered entity participating in an OHCA that performs a function or activity set forth in the definition of a business associate.8 Therefore, the entities that participate in an OHCA may share PHI for the joint health care activities of the OHCA without entering into BAAs with each other.

D. OHCA participants may use a joint notice of privacy practices so long as:

i. The participants agree to abide by the notice with respect to information created or received as part of its participation;

---

7 45 C.F.R. § 164.506(b)(5).
8 45 C.F.R. § 160.103.
ii. The content and delivery of the joint notice complies with the requirements set forth at 45 C.F.R. § 164.520(b) and (c) (general content and delivery requirements for notices of privacy practices). Provision of the joint notice by any participant will satisfy the requirements for all other participants;

iii. The joint notices describes with reasonable specificity the covered entities or class of covered entities and the service delivery sites or classes of sites to which it applies; and

iv. The joint notice states, if applicable, that the participants will share PHI with each other as necessary to carry out treatment, payment or health care operations relating to the OHCA.  

E. The regulations do not require formal documentation of OHCA designation. If the participants are using a joint notice, they should consider documentation of acceptable of the form notice and agreement to follow its terms.

F. Although there are not provisions regarding joint liability, participants should consider whether to impose certain standard safeguards and procedures because they are sharing information and could all be implicated in the event of an unauthorized access or use of information being shared among the participants.

II. Risk Assessment and OCR Audits

2.1 The Security Rule requires that covered entities (and, per HITECH, business associates) conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the entity.  

2.2 To the extent that a covered entity has conducted a risk assessment, it is recommended that an annual GAP analysis be completed in order to address the often changing risks associated with the use of technology associated with the provision of health care services and the management of a covered entity’s business.

2.3 Within the past 12 months, it has become clear that OCR is no longer only taking enforcement action against large covered entity providers. Where a physician practice has been the subject of an OCR investigation, the practices’ failure to have conducted a Security Rule risk assessment appears to be OCR’s most significant concern. Conducting a risk assessment (or having one conducted by an objective third party) almost necessarily involves the use of significant resources. With that said, it has never been more apparent that a risk assessment is the cornerstone to Security Rule compliance. Importantly, to the extent a risk assessment is conducted through a third party, it is highly recommended to engage the third party vendor through legal counsel so as to maintain attorney-client privilege with regard discussions and

---

9 45 C.F.R. § 164.520(d).
10 45 C.F.R. § 164.308(a)(1)(ii)(a).
findings associated with the drafting of the final assessment (which assessment, however, would be a document provided to OCR upon its request).

2.4. Practical considerations associated with conducting a risk assessment include asking the following questions:

A. Have you identified the e-PHI within your organization?\textsuperscript{12}

B. What are the external sources of e-PHI? For example, do vendors or consultants create, receive, maintain or transmit e-PHI?

C. What are the human, natural, and environmental threats to information systems that contain e-PHI?

2.5. **Important Associated Definitions.** Unlike “availability,” “confidentiality,” and “integrity,” there are some important terms within the context of conducting a risk assessment that are not expressly defined in the Security Rule. The following definitional considerations, which are consistent with common industry definitions, are provided to help contextualize the risk assessment endeavor.

A. **Vulnerability.** Vulnerability is defined in NIST Special Publication (SP) 800-30 as “[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.” Vulnerabilities, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as inappropriate access to or disclosure of e-PHI. Vulnerabilities are often grouped into two general categories: technical and non-technical. Technical vulnerabilities may include: holes, flaws or weaknesses in the development of information systems; or incorrectly implemented and/or configured information systems. Non-technical vulnerabilities may include ineffective or non-existent policies, procedures, standards or guidelines.

B. **Threat.** An adapted definition of threat, from NIST SP 800-30, is “[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.” There are several types of threats that may occur within an information system or operating environment. Threats may be grouped into general categories such as natural, human, and environmental. Examples of common threats include: (1) Natural threats such as floods, earthquakes, tornadoes, and landslides; (2) Human threats, which are enabled or caused by humans and may include intentional (e.g., network and computer based attacks, malicious software upload, and unauthorized access to e-PHI) or unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions; and (3) Environmental threats such as power failures, pollution, chemicals, and liquid leakage.

C. **Risk.** Risk can be understood as a function of (1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and (2) the resulting impact on the organization if the threat manifests through a security incident or breach. This means that risk is

\textsuperscript{12} This includes e-PHI that you create, receive, maintain or transmit.
not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.

2.6. **Risk Assessment Considerations.** There are numerous methods of performing risk analysis and there is no single method or “best practice” that guarantees compliance with the Security Rule.

   A. Within the scope of a risk assessment, the Security Rule includes the potential risks and vulnerabilities to the confidentiality, availability and integrity of all e-PHI that an organization creates, receives, maintains, or transmits.\(^\text{13}\) This includes e-PHI in all forms of electronic media, such as hard drives, CDs, DVDs, flash drives, or other storage devices, personal digital assistants, transmission media, or portable electronic media. Electronic media includes a single workstation as well as complex networks connected between multiple locations. It is important for covered entity’s to take into account all of its e-PHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its e-PHI.

   B. Identify where the e-PHI is stored, received, maintained or transmitted. An organization could gather relevant data by: reviewing past and/or existing projects; performing interviews; reviewing documentation; or using other data gathering techniques. The data on e-PHI gathered using these methods must be documented.\(^\text{14}\)

   C. Identify and document reasonably anticipated threats to e-PHI.\(^\text{15}\) Covered entities should also identify specific threats that are unique to the circumstances of their environment. Furthermore, it is important to identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI.\(^\text{16}\)

   D. Assess and document the (a) security measures it uses to safeguard e-PHI, (b) whether security measures required by the Security Rule are already in place, and (c) if current security measures are configured and used properly.\(^\text{17}\) The security measures implemented to reduce risk will vary among covered entities. For example, small covered entities tend to have more control within their environment and likely have fewer variables (e.g., fewer workforce members and information systems) to consider when making decisions regarding how to safeguard e-PHI. As a result, the appropriate security measures that reduce the likelihood of risk to the confidentiality, availability and integrity of e-PHI in a smaller covered entity may differ from those that are appropriate in larger covered entity.

   E. Take into account the probability of potential risks to e-PHI.\(^\text{18}\) The results of this assessment, combined with the initial list of threats, will influence the determination of which threats the Security Rule requires protection against because they are “reasonably

---

13 45 C.F.R. § 164.306(a).
14 45 C.F.R. § 164.308(a)(1)(ii)(A), 164.316(b)(1).
17 45 C.F.R. 164.306(b)(1), 164.308(a)(1)(ii)(A), 164.316(b)(1).)
Importantly, covered entities should maintain documentation of all threat and vulnerability combinations along with the associated likelihood that such threats and vulnerabilities may impact the confidentiality, availability and integrity of e-PHI of an organization. 19

F. Consider the “criticality,” or impact, of potential risks to confidentiality, integrity, and availability of e-PHI. 20 A covered entity must assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability. A covered entity may use any combination of a qualitative or quantitative to measure the potential impact. Resulting from this assessment should be the documentation of all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of e-PHI within the covered entity. 21

G. Assign risk levels for all threat and vulnerability combinations identified during the risk assessment. The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination might be performed by assigning a risk level based on the average of the assigned likelihood and impact levels. Covered entities must document the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level. 22

H. The Security Rule requires the risk assessment to be documented but does not require a specific format. 23 In order for a covered entity to update and document its security measures “as needed,” which the Security Rule requires, it should conduct continuous risk assessment to identify when updates are needed. 24 Although the Security Rule does not specify how frequently to perform risk assessments as part of a comprehensive risk management process, to some extent it should be an on-going process. The frequency of performance will vary among covered entities; some covered entities may perform these processes annually or as needed depending on circumstances of their environment.

2.7. HHS/OCR Audits.

A. Section 13411 of the HITECH Act requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the Privacy and Security Rules and Breach Notification standards. To implement this mandate, OCR piloted a program to perform 115 audits of covered entities to assess privacy and security compliance. Audits conducted during the pilot phase began November 2011 and concluded in December 2012.

B. Audits are not “intended” to trigger enforcement action.

23 45 C.F.R. 164.316(b)(1).
24 45 C.F.R. 164.306(e), 164.316(b)(2)(iii).
C. Currently, the audit protocol covers 169 areas of performance evaluation, including 81 related to the Privacy Rule, 10 related to the Breach Notification Rule, and 78 related to the Security Rule.

D. The audit protocol is available at the HHS OCR Privacy website, and provides an integrated description of key regulation components.25

III. Responding to Patient Complaints and Office for Civil Rights (OCR) Inquiries

3.1 Patient Complaints

A. The HIPAA Privacy regulations require that a covered entity have a process for individuals to make complaints regarding its policies and procedures or its compliance with HIPAA.26

i. The covered entity must also document all complaints and their disposition.27

ii. This documentation must be maintained for 6 years from its creation.28

B. A covered entity should determine whether it has other patient complaint or grievance policies that must be considered and followed when responding to a patient’s complaint.

C. The covered entity’s Notice of Privacy Practices must inform individuals that they may make complaints to the provider and to the Secretary of HHS if they believe their privacy rights have been violated, briefly describe how to make a complaint to the covered entity and state that the individual will not be retaliated against for filing a complaint.29

D. Practical considerations when responding to patients:

i. Train all employees to notify privacy officer of all complaints or concerns expressed by patients related to the privacy and security of patient information, even if a formal complaint is not lodged.

ii. Document all conversations with complainant. Often a conversation is needed in order to gather facts necessary for further investigation.

iii. Watch disclosure of sensitive employee information, including the employee’s name, when discussing a complaint/ incident with patients.

25 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

26 45 C.F.R. § 164.530 (d)(1).
27 45 C.F.R. § 164.530 (d)(2).
28 45 C.F.R. § 164.530 (j).
29 45 C.F.R. § 164.520 (b)(1)(vi).
iv. Documentation should include subject of complaint, how investigated (who conducted, what was involved, findings), remedial measures (or if none, then basis for decision) and efforts to mitigate.

v. Consider whether a written breach notice is required under the HITECH Act (or state law).

3.2 OCR Inquiries

A. The OCR enforces the HIPAA Privacy and Security Rules. As part of that enforcement activity, it investigates complaints from individuals.

B. A person who believes that a covered entity is not complying with HIPAA may file a complaint.\(^\text{30}\)

i. The complaint must:

1. Be filed in writing, either on paper or electronically;

2. Name the person who is the subject of the complaint and describe the acts or omissions believed to be in violation of HIPAA; and

3. Be filed within 180 days of when the complainant knew or should have known that the act or omission occurred (although this time limit can be waived for “good cause”).\(^\text{31}\)

ii. Additional procedures may be developed, such as for the place and manner of filing, by Federal Register notice.\(^\text{32}\)

iii. Complaints may be investigated, including a review of policies, procedures and practices of the covered entity. The initial written communication must describe the act(s) or omission(s) that are the basis of the complaint.\(^\text{33}\)

C. A covered entity must cooperate with investigations and compliance reviews of its policies, procedures and practices to determine whether it is complying with HIPAA.\(^\text{34}\)

D. For its investigation, OCR generally requests written, narrative responses to a list of questions as well as supporting materials, such as copies of relevant policies and procedures and training logs and materials. The questions often relate to the covered entity’s investigation of the incident and remedial actions taken, but also inquire about broader HIPAA compliance matters with respect to the covered entity, including responses to prior HIPAA complaints.

\(^{30}\) 45 C.F.R. § 160.306(a).

\(^{31}\) 45 C.F.R. § 160.306(b).

\(^{32}\) 45 C.F.R. § 160.306(b).

\(^{33}\) 45 C.F.R. § 160.306(c).

\(^{34}\) 45 C.F.R. § 160.310 (b).
E. “Informal resolution”: The OCR has sent letters to covered entities that have been the subject of a complaint indicating that it closed the subject complaint and has determined to resolve the matter “informally” by providing technical assistance.

   i. Letters cite OCR authority seek cooperation of covered entities and business associates with compliance and to provide technical assistance\(^ {35}\) and include information about privacy and security rule requirements related to the subject of the underlying complaint.

   ii. Letter encourages covered entity to assess and determine if any incident of noncompliance and if so, take steps to ensure that there is not a recurrence. Also, the letter requests that the covered entity respond in writing within 60 days explaining the action taken to resolve the claims. The OCR reserves the right to take further action if a response is not received or the response is “inadequate”.

F. Imposition of Civil Monetary Penalties: Cignet Health of Prince George’s County (Maryland)

   i. 38 complaints were filed with the OCR for failure to provide 41 patients access to their records upon request, which resulted in civil monetary penalty of $1,351,600.\(^ {36}\)

   ii. The Proposed Determination outlines Cignet’s failure to cooperate with the OCR’s investigation, including:

      1. Refusal to respond to repeated demands to produce records;

      2. Failure to produce records in response to a subpoena until the OCR filed a petition to enforce subpoena in U.S. District Court and and obtained default judgment;

      3. When Cignet then produced records, the materials provided included medical records for approximately 4,500 other individuals not covered by the OCR’s requests or demands.

      4. OCR found that failure to cooperate was due to “willful neglect” and imposed a $3 million civil monetary penalty for those violations.\(^ {37}\)

   iii. This penalty was first civil monetary penalty imposed for a HIPAA Privacy Rule violation and was calculated using increased penalty amounts authorized by HITECH Act.\(^ {38}\)

\(^{35}\) 45 C.F.R. § 160.304.


\(^{37}\) Id.

\(^{38}\) Id.
G. Practical considerations when responding to OCR inquiries:

i. Be clear, thorough and accurate, but expect follow-up requests.

ii. Consider range of remedial actions, such as training, revisions to policies, employee sanctions, and providing breach notices (especially if more than one patient involved).

iii. Assess status of compliance in general and take measures promptly as necessary to address identified issues. The OCR is not limited to investigating only the issues that gave rise to the patient complaint/OCR inquiry. Instead, OCR may look beyond the actual incident reported to determine underlying cause, such as investigating whether particular safeguards or processes were lacking or if there is a systemic failure by the covered entity.

IV. WORKFORCE TRAINING

4.1. Although maintain policies and procedures related to a covered entity’s obligations under the Privacy, Security, and Breach Notification Rules is a significant aspect to HIPAA compliance, the extent to which a covered entity’s workforce understands what is expected of them is, in many regards, the most critical component of compliance efforts.

4.2. The Privacy Rule specifically requires that a covered entity must train all members of its workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.\\(^39)\\

4.3. Significantly, the content of workforce training is left within a covered entity’s discretion.\\(^40)\\ That being said, it is advisable for a covered entity to specifically train its workforce with regard to its unique privacy and security requirements and considerations. Though “off the shelf” training likely includes all of the elements of HIPAA privacy and security should be contained in training, if the training is not specifically tailored to a particular covered entity, there is more of a likelihood that an issue with regard to compliance may arise.

4.4. In its commentary, OCR has specifically stated that retraining is not technically required other than in the case of material changes to the privacy policies and procedures of the covered entity.\\(^41)\\ Training is “required” for each new member of the workforce within a “reasonable period of time” after the person joins the covered entity’s workforce, as well as To each member of the covered entity’s workforce whose functions are affected by a material change in the policies or procedures within a “reasonable period of time” after the material change becomes effective.\\(^42)\\ However, best practices with regard to training suggest that training for the workforce should additionally occur on an annual basis, as well as for individuals shortly after their date of hire.

---


\(^{39}\) 45 CFR § 164.530(b)(1).


\(^{41}\) 45 C.F.R. § 164.530(b); 65 Fed. Reg. 82745 (December 28, 2000).

\(^{42}\) 45 C.F.R. § 164.530(b)(2)(i).
4.5. Documentation of workforce members’ participation in training is key.\textsuperscript{43} Although OCR does not require a covered entity to evidence training through collection of workforce members’ signatures, it is critical that covered entities are able to demonstrate to OCR in a meaningful and incontrovertible way that training has occurred. Additionally, OCR requires that covered entities must maintain written or electronic records that training has occurred for a period of six years after the training has occurred.\textsuperscript{44}

V. Hot Technology-Related Topics in HIPAA Compliance

5.1. Email.

A. Covered entities may utilize email when communicating with each other and patients. Nothing in HIPAA prohibits the use of email. That being said, it is \textit{how} a covered entity uses email that is potentially problematic.

B. Simply said, encrypted email is your best bet.

C. Web-based email may not necessarily be HIPAA compliant.

D. Best practices, in terms of “minimum necessary” considerations, should always be employed.

E. Be sure you know to whom you are sending an email.

5.2. Text Messaging.

A. From a compliance perspective, text messaging may provide more challenges than email from a security perspective.

B. If use is “necessary,” limit message content as much as possible.

C. As with email, it is important to consider whether these messages should be considered part of the patient record.

5.3. Mobile Devices.

A. The use of mobile devices by health care providers is here to stay. As a result of this new constant, it is important for covered entities to understand both the benefits and risks to the use of such technology.

B. There are many resources available to assist with the compliant use of mobile devices. Two examples are below.

i. The Office for the National Coordinator of Health Information Technology: Mobile Devices Roundtable: Safeguarding Health Information.

\textsuperscript{43} 45 C.F.R. § 164.530(b)(2)(ii); 65 Fed. Reg. 82745 (December 28, 2000).

\textsuperscript{44} 45 C.F.R. 164.530(j).
ii. Joint OCR/Office for the National Coordinator of Health Information Technology Initiative: Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information


iii. A slightly older, yet still relevant 2006 HHS Security Guidance

www.hhs.gov/ocr/privacy/hipaa/.../securityrule/remoteuse.pdf

C. If a covered entity allows workforce members to use their own devices (i.e., a BYOD program), it is critical to have an associated policy that all such workforce members understand.

5.4. Social Media.

A. Covered entities should have a clear policy regarding workforce members’ use of social media. This policy should be driven by privacy considerations, as well as the Security Officer’s logistical determinations on “outside” website access.

B. Because mobile devices will almost certainly include a camera and video camera, a covered entity’s exposure associated with a workforce member’s ability to post photos and videos containing PHI should be addressed as policies and procedures are developed.

5.5. Cloud Vendors.

A. The manner in which a covered entity utilizes a cloud vendor will determine whether the vendor is a business associate. A key consideration here is whether the cloud vendor will have unfettered access to the PHI stored “on the cloud.”

B. Although stakeholders are hoping that a final HITECH regulations with explicitly address when a cloud vendor is a business associate, it will ultimately be important for covered entities to have a clear appreciation of the flow of their PHI when deciding whether to require the execution of a business associate agreement.

VI. Marketing and the Sale of PHI

6.1 In contrast to how marketing considerations were addressed pre-HITECH, the HITECH Final Rule requires authorizations for all health care operations and treatment communications where the covered entity receives financial remuneration for making the communication from a third party whose products or services are being described. 45 Under the pre-HITECH Privacy Rule, treatment and certain health care operations communications were

45 78 Fed. Reg. at 5595.
specifically excluded from the definition of “marketing.” Those same exceptions are no longer applicable if in exchange for making the communication, the covered entity receives financial remuneration from a third party. Importantly, as was the case pre-HITECH, no authorization is required to make a treatment or health care operations communication (or other marketing communication) if the communication is made face-to-face or consists of a promotional gift of nominal value.

6.2 Under the HITECH Final rule, “financial remuneration” is defined as “direct or indirect payment from or on behalf of a third party whose product or service is being described,” but does not include payments for the actual treatment of the individual. Indirect payments refer to payments that flow from an entity on behalf of the third party whose product or service is being described to the covered entity. Notably, financial remuneration does not include non-financial, in-kind benefits; instead, it is limited to actual monetary payments. For example, a third party may provide a covered entity with in-kind goods, such as written materials, that describe the third party’s products or services. The covered entity may then distribute those materials to its patients for the purpose of recommending the third party’s product or service as an alternative treatment without obtaining an authorization. By contrast, if the covered entity also receives a monetary payment from the third party for the purpose of making the communication, then an authorization is required.

6.3 Importantly, for financially remunerated treatment and health care operations communications that will require an authorization under the Final Rule, the scope of the authorization need not be limited to communications describing a single product or service or the products or services of a single third party. Instead, authorizations may apply to subsidized communications generally, provided that the authorization adequately describes the intended purposes of the requested uses and disclosures. Such authorizations must also disclose the fact that the covered entity is receiving financial remuneration from a third party.

6.4 Going forward, covered entities will need to answer two important questions prior to using or disclosing PHI for treatment or health care operations communications that involve the receipt of financial remuneration from a third party: (1) whether the covered entity is receiving “financial remuneration” as defined by the Privacy Rule, and (2) whether the covered entity is receiving the financial remuneration for the purpose of making the communication.

6.5 OCR has also provided what is referred to as the “refill reminder” exception to the marketing prohibition. This exception clarifies that the following communications are permitted without the need for a marketing authorization:

- Communications regarding generic equivalents of a currently prescribed drug;
- Communications that encourage individuals to take their prescribed medication as directed; and

---

46 45 C.F.R. § 164.501 (defining “marketing”).
49 Id. at 5596.
• For individuals who are prescribed a self-administered drug or biologic, communications regarding all aspects of a drug delivery system.\(^{50}\)

6.6 While a covered entity may receive financial remuneration in exchange for making these communications and still remain within the marketing exception, such remuneration must be limited to the covered entity’s costs for making the communication. Permissible costs include only the costs of labor, supplies, and postage. Where a covered entity generates a profit or receives payment for other costs in exchange for making a prescription refill reminder, the exception would not apply and the covered entity must obtain individual authorization prior to using or disclosing PHI in furtherance of the communication.\(^{51}\) Additionally, OCR has provided additional guidance with regard to the application of the refill reminder exception, which is located here: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/marketingrefillreminder.html.

VII. Breach Notifications and Reporting Requirements

7.1 **Background:** Prior to the HITECH Act, no federal law mandated that individuals be informed in the case of improper use or disclosure of their PHI.

7.2 **Section 13402 of the HITECH Act** creates a federal breach notice and reporting requirement for covered entities.\(^{52}\)

A. A covered entity that “access, maintains, retains, modified, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information” must “notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed” due to a breach.\(^{53}\)

B. In addition, business associates must notify covered entities of breaches.\(^{54}\)

7.3 **HITECH Act Breach Definition:** Section 13400 of the HITECH Act defines “breach” as the “unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information”, subject to 3 exceptions (as discussed below).\(^{55}\)

7.4 **Interim Final Rule:** On August 24, 2009, the OCR issued an interim final rule regarding the HITECH Act’s notice and reporting requirements, which was effective on September 23, 2009.\(^{56}\) The Interim Final Rule provided detail regarding the definitions used in the breach requirements, application of the harm threshold and provision of notices.

---

\(^{50}\) *Id.* at 5596.

\(^{51}\) *Id.* at 5596–97.

\(^{52}\) codified at 42 U.S.C. § 17932.

\(^{53}\) 42 U.S.C. § 17932(a).

\(^{54}\) 42 U.S.C. § 17932(b).


\(^{56}\) 74 Fed. Reg. 42740.
7.5 **Unsecured PHI:** The breach notifications and reporting apply only to “unsecured protected health information”, which is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services.57

A. The HITECH Act directs that the HHS website will set forth information on these approved technologies.58

B. Note that encryption is not required.

7.6 **Determination that Breach Has Occurred:** In order to constitute a “breach”, the use or disclosure of unsecured PHI must satisfy three requirements:

A. There has been an “unauthorized” acquisition, access, use or disclosure of protected health information; and

B. The use or disclosure compromises the security or privacy of protected health information; and

C. An exception does not apply.

7.7 **Unauthorized Uses and Disclosures:** A use or disclosure of PHI is “unauthorized” if it is not permitted under the HIPAA Privacy Standards.59

A. Not all violations of the HIPAA Privacy Standards constitute an unauthorized use or disclosure, such as violations of the administrative requirements related to training and reasonable safeguards.

B. Uses and disclosures that impermissibly involve more than the minimum necessary information are unauthorized and therefore may constitute a breach.

7.8 **Exceptions to Breach Definition:** The following three exceptions to the definition of “breach” are provided in the definition of breach as defined in the HITECH Act:

A. An unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of the covered entity or one of its business associates if the use were made in good faith, within the course and scope of employment or other professional relationship and does not result in further uses or disclosures not permitted by the HIPAA Privacy Standards;

B. An inadvertent disclosure by a person who is authorized to access PHI at the covered entity or one of its business associates to another person authorized to access PHI at the covered entity or one of its business associates or organized health care arrangement in which

58 HITECH Act § 13402(h)(2), codified at 42 U.S.C. § 17932(h)(2)). The current information is included in the Interim Final Rule at 74 Fed. Reg. 42742–42743 and the OCR’s website in the “Breach Notification Section”.
the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by the HIPAA Privacy Standards; or

C. A disclosure where the covered entity or one of its business associates has a good faith belief that an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.  

7.9 **Risk Assessment Factors under the Interim Final Rule:** Under the Interim Final Rule, a use or disclosure “compromises the security or privacy of protected health information” if it poses a significant risk of financial, reputational or other harm to the individual. The preamble to the Interim Final Rule addressed a number of factors may be considered in making this determination, including:

A. Who impermissibly used or to whom the information was impermissibly disclosed (for example, if the information is disclosed to another covered entity, there may be less risk because that entity is obligated by HIPAA to protect the information);

B. If the covered entity were able to take immediate steps to mitigate an impermissible use or disclosure which would eliminate or reduce the risk of the harm to the individual to less than a significant risk (for example, the recipient might sign a confidentiality agreement assuring that it will not further use or disclose the information);

C. If the PHI were returned prior to being accessed for an improper purpose (for example, if a stolen laptop is returned and forensic analysis establishes that the information was not opened, altered, transferred or compromised);

D. The type and amount of PHI involved in the impermissible use or disclosure (for example, if the information only includes patient name and fact that healthcare services were received from a hospital, without more information, then there may not be a significant risk of harm);

E. Whether the information increases the risk of identity theft (for example, the information includes social security number, account number or mother’s maiden name); and

F. If the use or disclosure involves a limited data set (as the term is used at 45 CFR § 164.514 (e)), then it must consider the risk of re-identification unless the limited data set does not include zip codes or dates of birth.

7.9 **Risk Assessment Factors under the Final HITECH Rule:** In the preamble to the Final HITECH Rule, OCR states that the Final HITECH Rule “modifies and clarifies the definition of breach and the risk assessment approach” set forth in the Interim Final Rule. It also notes that the language in the Interim Final Rule and its preamble “could be construed and

---

60 HITECH Act § 13400 (1)(B), codified at 42 U.S.C. § 17921 (1)(B); see also 45 C.F.R. § 164.402.
61 45 C.F.R. § 164.402.
implemented in manners we had not intended”, and so the HITECH Final Rule is intended to provide a more uniform and objective test for determining if a breach has in fact occurred.63

A. The Final HITECH Rule provides that an acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA Privacy Standards is presumed to be a breach.

B. The presumption may be rebutted if the covered entity (or business associate) demonstrates that there is a “low probability” that PHI has been “compromised” after conducting (and documenting) a risk assessment that consists of at least the following factors:

   i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

   ii. The unauthorized person who used the PHI or to whom the disclosure was made;

   iii. Whether the PHI was actually acquired or viewed; and

   iv. The extent to which the risk to the PHI has been mitigated.64

C. The term “compromise” is not defined in the HITECH Final Rule.

D. In the preamble to the Final HITECH Rule, the OCR states that it intends to issue additional guidance on performing risk assessments, but this guidance has not been released yet.65

7.10 **Practical Considerations:**

A. Utilize a committee to determine if risk assessment results in a breach determination: allows for input from more people and prevents blame falling on single person if issues arise later.

B. Be consistent with respect to process and documentation to extent possible.

C. Determine whether will advise liability carrier of incident.

D. When drafting notices:

   i. Clarity is important so that notice is effective without raising potentially unnecessary concerns.

   ii. Describe what was and what was not disclosed.

---

63 Id.
64 Id. at 5641-5643; 45 C.F.R. § 164.402.
iii. Be certain that person(s) listed as contact for follow up information has information necessary to respond to inquiries.

iv. Be prepared to provide media notice or substitute notice if required.

E. Notice to Secretary:

i. When completing online notice submission form, be certain to provide thorough information; do not view as an informal communication.

ii. Breach notices have been the source of numerous enforcement actions, including recent action involving Hospice of North Idaho.66

iii. If less than 500 individuals affected, maintain log of breaches and create system for annual reminders to submit form by deadline (due no later than 60 days after the end of each calendar year).

F. Remember to consider mitigation obligation under Privacy and Security Rules even if do not provide notices.

G. If improper use or disclosure but decide that notice is not required, the covered entity still should take steps to address underlying issue and document all measures taken (i.e., training, audits, revised policies and procedures, additional security measures, implementation of encryption, imposition of sanctions).

i. This step may prevent future issues that might require notices.

ii. If government does not agree with assessment, these steps will be helpful evidence that took incident seriously and carefully considered decision.

7.11 State Law Reporting Requirements

A. State law reporting requirements are not preempted and may impose different deadlines and notice requirements, as well as require disclosure to state agencies, so covered entities must analyze these obligations as well.

B. Notably, some state laws do not include a risk assessment and require reporting for all uses or disclosures that satisfy statutory definition of breach.

7.12 Business Associate Issues: Bear in mind that a covered entity may also be a business associate.

A. Be aware of reporting obligations from role as Business Associate—who decides if there is a breach?

---

66 Resolution Agreement between United States Department of Health and Human Services and, Office for Civil Rights and Hospice of North Idaho, see http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/honi-agreement.pdf.
B. When negotiating Business Associate Agreements, review breach notification provisions carefully to determine how costs of notices and other reporting and notice responsibilities are allocated.

VIII. Business Associate “Management”

8.1 Especially with the advent of HITECH (whereby business have direct regulatory obligations under HIPAA), covered entities may find that the negotiation of BAAs will become more challenging. Regardless of a covered entity’s size and the extent to which vendors/BAs have access to or utilize and create PHI, it is important for the covered entity to have an accurate sense of who their BAs are and to what extent the covered entity has regulatory exposure if a breach occurs at the business associate level.

8.2 The HITECH Final Rule expanded the universe of vendors that are considered business associates. Now, all subcontractors of a business associate are now considered to be business associates themselves. With this change, there may be push back from such vendors regarding whether they are, in fact a business associate. Additionally, an unintended consequence of the expanded regulatory reach may be an increase in cost associated with services provided by business associates and their subcontractors.

8.3 Indemnification provisions and notification requirements in BAAs may vary and require increasing negotiation, and regardless of what a particular BAA contains in this regard, it is important for a covered entity to maintain a database that contains all business associate agreements. To the extent a problem arises, a covered entity is in a much better position from the outset if it is able to address issues involving a business associate specific to that business associate’s contractual obligations.

8.4 Covered entities should consider the extent to which utilizing a particular vendor (in a business associate capacity) overshadows the potential exposure associated with that business associate’s access, use, or creation of PHI. For example, if a potential business associate will not indemnify the covered entity for losses associated with a breach caused by the business associate, it may be that the covered entity decides not to engage that particular vendor. In an effort to streamline these considerations, covered entities may want to give thought to their overall risk tolerance as it relates to business associates generally so that these issues are not discussed only with regard to a particular BAA negotiation.

8.5 There is much debate (and often hotly contested negotiation) regarding whether a covered entity should or may be required to, oversee or “audit” its business associates with regard to HIPAA compliance. The extent to which this occurs (and reflected in the associated BAAs) is directly related to the associated negotiating power of each entity. Covered entities that request this ability should consider their ability to conduct these audits and what in fact they will do with the information obtained.

A. Additional related considerations include whether the covered entity will have the authority to impose additional safeguards, policies or procedures in response to audit findings.
B. The parties may consider permitting a third party to conduct an audit or having the business associate share the results of its periodic audits.

C. What other steps might help covered entity feel comfortable with vendor’s compliance—diligence questionnaire? Management interviews?

D. Covered entities should consider other risks to right to conduct audit, including whether it strengthens argument that business associate is an agent of the covered entity. Under the HITECH Final Rule, covered entities are liable for civil monetary penalties based on the acts or omissions of their agents, including workforce members or business associates, acting within the scope of the agency. 67

8.6 Covered entities need to develop a plan for implementing business associate agreements that comply with HITECH Final Rule requirements by the applicable deadlines.

A. The HITECH Final Rule grandfathered BAAs that were in effect as of January 25, 2013 (the date the HITECH Final Rule was published) and that complied with the existing BAA requirements as of that date so long as the BAA was not renewed or modified during the period from March 26, 2013 through September 23, 2013. 68

B. These grandfathered agreements are deemed compliant until the earlier of the date of renewal or modification or September 22, 2014. 69

C. Note that the grandfather period only extends the date of compliance with the requirements for written agreements but does not extend the compliance date for other aspects of the HITECH Final Rule.

IX. Proposed Changes to Accounting Requirement and Access Report

9.1 HITECH Act Statutory Changes. Section 13405 (c) of the HITECH Act states that a covered entity include uses and disclosures for treatment, payment and health care operations in an accounting made through an “electronic health record”. 70 “Electronic health record” is defined as an “electronic health record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.” 71

9.2 Proposed Accounting Rule. The OCR issued a proposed rule on May 31, 2011 to expand the accounting provision to provide individuals with the right to receive an “access report” indicating who has accessed electronic PHI in a designated record set and to make changes to the existing accounting requirements under the HIPAA Privacy Rule. 72

9.3 Changes to Accounting Requirement. The Proposed Accounting Rule would:

67 45 C.F.R. § 160.402(c).
68 45 C.F.R. § 164.532(c).
69 Id.
70 codified at 42 U.S.C. § 17935 (c).
71 Section 13400 (5) of the HITECH Act, codified at 42 U.S.C. § 13400 (5).
A. Limit scope to disclosures of PHI that must be included to disclosures of PHI in a designated record set.\textsuperscript{73} This change would align the information subject to the right to an accounting with the rights to access and amendment.

B. Require that the accounting include disclosures by business associates.\textsuperscript{74}

C. Reduce the required timeframe of disclosures that must be included from 6 years (as currently required) to 3 years.\textsuperscript{75} In the preamble to the Proposed Rule, the OCR notes its belief that individuals generally are most interested in recent disclosures.\textsuperscript{76}

D. List the kinds of disclosures that must be included in an accounting, rather than take the approach of listing what does not have to be included, as currently set forth in the HIPAA Privacy Rule.\textsuperscript{77}

E. Modify the content of the accounting, including the manner in which disclosures may be described and the ability of an individual to limit the request to a specific time period, type of disclosure or recipient.\textsuperscript{78}

F. Require that the accounting be provided within 30 days of the request (rather than current 60 day timeframe), with a possible extension of an additional 30 days.\textsuperscript{79}

9.4 Right to an Access Report.

A. In the Proposed Accounting Rule, the OCR proposes to provide individuals with the right to receive a written access report that indicates who has accessed PHI about the individual in an electronic designated record set maintained by the covered entity or business associate for up to 3 years prior to the date on which the access report is requested.\textsuperscript{80}

B. The report must contain the following information:

   i. Date of access.

   ii. Time of access.

   iii. Name of person, if available, otherwise name of entity accessing the electronic designated record set.

   iv. Description of what information was accessed, if available.

\textsuperscript{73} Proposed 45 C.F.R. § 164.528 (a) (1)
\textsuperscript{74} Id.
\textsuperscript{75} Id.
\textsuperscript{76} 76 Fed. Reg. at 31430.
\textsuperscript{77} Proposed 45 C.F.R. § 164.528 (a)(1).
\textsuperscript{78} Proposed 45 C.F.R. § 164.528 (a)(2).
\textsuperscript{79} Proposed 45 C.F.R. § 164.528 (a)(3).
\textsuperscript{80} Proposed 45 C.F.R. § 164.528 (b)(1).
v. Description of action by the user, if available (i.e., create, modify, access or delete).\textsuperscript{81}

C. Individuals must have the right to limit the report to a specific date, time period or person.\textsuperscript{82}

D. The report’s format must be understandable to the individual.\textsuperscript{83}

E. Covered entities have 30 days to provide the report, with the ability to extend by one 30-day period.\textsuperscript{84}

9.5 \textbf{Practical Considerations.}

A. The HITECH Final Rule did not address the Proposed Accounting Rule.

B. Providers can begin to contact their electronic health record vendors to discuss steps being taken to prepare for new obligations.

C. The changes when issued will result in changes to a covered entity’s Notice of Privacy Practices. Providers will not be able to include these revisions when making other HITECH Act-driven revisions, covered entities may want to be conservative when printing or ordering new NPPs.

\textsuperscript{81} Proposed 45 C.F.R. § 164.528 (b)(2).
\textsuperscript{82} Proposed 45 C.F.R. § 164.528 (b)(2)(ii).
\textsuperscript{83} Proposed 45 C.F.R. § 164.528 (b)(2)(iii).
\textsuperscript{84} Proposed 45 C.F.R. § 164.528 (b)(3)(i).