Contents

(Some words in the Security Rule Primer are capitalized because they have a special HIPAA definition quickly found by using *The HIPAA E-Tool®* Search Box.)

I. The Privacy Rule – The Fundamental HIPAA Rule

The Privacy Rule[1] is the fundamental HIPAA Rule because it:

1. Applies to all Protected Health Information (PHI) maintained or transmitted in any form or medium;[2]
2. Establishes Permitted and Required Uses and Disclosures of PHI for both Covered Entities and Business Associates;[3] and
3. Establishes special, specific rights Individuals have concerning their own PHI.[4]

GUIDANCE NOTE – The Privacy Rule is the Basis for Security and Breach Notification Rules

Uses and Disclosures of PHI permitted or required by the Privacy Rule are the subject of both the Security and Breach Notification Rules.

The Security Rule

The Security Rule requires Covered Entities and Business Associates to protect against Uses and Disclosures of PHI not permitted or required by the Privacy Rule that is transmitted by Electronic Media or maintained in Electronic Media.[5]

The Breach Notification Rule

The Breach Notification Rule, applicable to both Covered Entities and Business Associates, defines "Breach" as the Acquisition, Access, Use or Disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the Security or Privacy of the PHI.[6]

II. Privacy Rule Overview

1. Standards and Implementation Specifications

The Privacy Rule is made up of Standards (rules concerning PHI[7]) and Implementation Specifications (instructions for implementing a Standard[8]) published in the Code of Federal Regulations. It is much longer than the Security Rule or Breach Notification Rule with internal references that interrupt its continuity.[9] Reference to the definition of "sale of protected health information" is incorrect adding to confusion.[10] This surely reflects the inclusive, intermittent process by which the Privacy Rule was developed and has been modified by the U. S. Department of Health and Human Services (HHS) since 1996 as directed by Congress.[11] *The*

[1] 45 CFR Part 160 and Subparts A and E of Part 164.
[2] 45 CFR § 164.500, 45 CFR § 160.103.
[3] 45 CFR § 164.502.
[4] See e.g. 45 CFR §§ 164.520-528.
[5] 45 CFR § 164.306, 45 CFR § 160.103.
[6] 45 CFR § 164.402.
[7] 45 CFR § 160.103.
[8] Ibid.
[9] 45 CFR §§ 164.500-534.
[10] See 45 CFR § 164.508(a)(4)(i), 45 CFR § 164.501, 45 CFR § 164.502(a)(5)(ii)(B).
[11] See, e.g.: 64 FR 59918, Nov. 3, 1999; 65 FR 82462, Dec. 28, 2000; 67 FR 14776, Mar. 27, 2002; 67 FR 53182, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 74 FR 4270, Aug. 24, 2009; 74 FR 56123, Oct. 30, 2009; 75 FR 40868, Jul. 14,

HIPAA E-Tool® re-arranged the order of Privacy Rule Standards and Implementation Specifications to present them logically according to their subject and make them easy to follow and implement.

2. Step-by-Step – Privacy Rule Compliance
   Privacy Rule Standards and Implementation Specifications are easy to follow when you know the steps. *The HIPAA E-Tool®* was created to untangle the Privacy Rule and present it in logical order with step-by-step Procedures and Forms.

III. Privacy Rule Standards and Implementation Specifications Covered in Section 4

Section 4 of *The HIPAA E-Tool®* covers Privacy Rule Standards and Implementation Specifications governing Individual Rights, Uses and Disclosures of PHI and most Administrative Requirements grouped as follows:

Part A – Rights of Individuals regarding their PHI
Part B – Uses and Disclosures of PHI
Part C – Administrative Requirements

IV. Privacy Rule Standards and Implementation Specifications in Other Sections

For clarity and ease of access some Privacy Rule Standards and Implementation Specifications are covered by Policies, Procedures and Forms in the following sections of *The HIPAA E-Tool®*:

1. Section 2, Basic HIPAA Policies
   HIPAA-1, HIPAA Compliance Program[12]
   HIPAA-2, Privacy Official[13]
   HIPAA-3, Security Official[14]
   HIPAA-4, Protected Health Information (PHI) and Electronic Protected Health Information (EPHI)[15]
   HIPAA-5, Parts 1, 2 and 3, Minimum Necessary Standard[16]
2. Section 7, Business Associates
   Privacy Rule Standards and Implementation Specifications regarding Covered Entities and Business Associates are grouped in Section 7, Business Associates and Policy BA-1, Business Associate Contract and Compliance Policy (Business Associate Agreement). They include the following Privacy Rule Standards and Implementation Specifications.
   A. A Covered Entity may Disclose PHI to a Business Associate and allow a Business Associate to create, receive, maintain, or transmit PHI on the Covered Entity's behalf, if it obtains "satisfactory assurances" in writing that the Business Associate will appropriately Safeguard the information.[17] "Satisfactory assurances" mean a written contract with the Business Associate (Business Associate Agreement – "BAA") that meets Privacy Rule requirements, or, if both Covered Entity and Business Associate are government entities, Other Arrangements (memorandum of understanding or other law and regulations) that accomplish the same objectives as a BAA.[18]
   B. The content that must be covered by a BAA or Other Arrangement is specified.[19]
   C. A Business Associate may Disclose PHI to a Business Associate that is a Subcontractor and allow the Subcontractor Business Associate to create, receive, maintain, or transmit protected health information on its behalf, if it obtains "satisfactory assurances" in writing that the Subcontractor Business Associate will appropriately Safeguard the information.[20] "Satisfactory assurances" obtained from a Subcontractor mean the same thing as

---

2010; 76 FR 31426, May 31, 2011; 78 FR 5566, Jan. 25, 2013; 78 FR 23872, Apr. 23, 2013; 79 FR 784, Jan. 7, 2014; 79 FR 7290, Feb. 6, 2014; 81 FR 382, Jan. 6, 2016 and 45 CFR §§ 164.500-534.

[12] 45 CFR § 164.530(c).
[13] 45 CFR § 164.530(a)(1).
[14] 45 CFR § 164.308(a)(2.
[15] 45 CFR § 164.502(a).
[16] 45 CFR § 164.502(b), 45 CFR §164.514(d).
[17] 45 CFR § 164.502(e)(1)(i); 45 CFR §164.502(e)(2).
[18] 45 CFR § 164.504(e); 78 FR 5600-1, Jan. 25, 2013.
[19] 45 CFR § 164.504(e).
[20] 45 CFR § 164.502(e)(1)(ii); 45 CFR §164.502(e)(2).

"satisfactory assurances" obtained by a Covered Entity from a Business Associate – a BAA or Other Arrangement meeting Privacy Rule requirements.[21] However, "satisfactory assurances" obtained from a Subcontractor must be as or more stringent than the permissible Uses and Disclosures of PHI that apply to the upstream Business Associate.[22]

D. A Subcontractor Business Associate must obtain the same written "satisfactory assurances" from its Subcontractor Business Associates as it provided to the upstream Business Associate "…no matter how far ''down the chain'' the information flows."[23]

E. Covered Entities and Business Associates that have credible evidence of a violation of the BAA by a Business Associate must investigate, take reasonable steps to end the violation and, if unsuccessful, terminate the BAA or Other Arrangement.[24] However, Covered Entities and Business Associates that are both government entities are not required to have language permitting termination of Other Arrangements if termination is inconsistent with their legal obligations as government entities.[25]

V. Administrative, Technical and Physical Safeguards required by the Privacy Rule

The Privacy Rule requires Covered Entities to have appropriate Administrative, Technical, and Physical Safeguards in place to protect the Privacy of PHI. **[26]** However, the Privacy Rule does not describe the Administrative, Technical, and Physical Safeguards it requires unlike the Security Rule that provides detailed Standards and Implementation Specifications for Administrative, Physical and Technical Safeguards.

1. <u>All Security Rule Safeguards are Safeguards required by the Privacy Rule</u>
   The Security Rule protects the same information as the Privacy Rule, however, the Security Rule only protects that information in Electronic form.[27] Electronic PHI is simply a subset of PHI[28] and the Privacy Rule covers all PHI.[29] Accordingly, Security Rule Administrative, Physical and Technical Safeguards to protect PHI transmitted by or maintained in Electronic Media by definition are among the Administrative, Technical, and Physical Safeguards required by the Privacy Rule to protect the Privacy of PHI. This is illustrated by an HHS 2012 Enforcement Rule Resolution Agreement.[30] Although the final Privacy Rule was published first, HHS was careful to ensure Security Rule requirements would work "hand in glove" with the Privacy Rule's Administrative, Technical, and Physical Safeguards.[31]
2. <u>Other Privacy Rule Administrative, Technical and Physical Safeguards</u>
   Privacy Rule Administrative, Technical, and Physical Safeguards besides Security Rule Safeguards are apparent from a review of HHS Enforcement Rule activities, Resolution Agreements and guidance published in the Federal Register or on the HHS Web Site. For example, HHS based Enforcement Rule Resolution Agreements on the following Privacy Rule Safeguards:
   A. Administrative Safeguards

---

[21] 45 CFR § 164.504(e)(5).
[22] 78 FR 5601, Jan. 25, 2013.
[23] 78 FR 5574, Jan. 25, 2013, 78 FR 5591, Jan. 25, 2013; 45 CFR §164.314(a), 45 CFR §164.502(e), 45 CFR § 164.504(e).
[24] 45 CFR § 164.504(e)(1)(ii)(iii); HITECH Act Section 13401(b), PL 111-5, Feb. 17, 2009; 78 FR 5597, Jan. 25, 2013; 65 FR 82641, Aug. 14, 2000.
[25] 45 CFR § 164.504(e)(3)(iii).
[26] 45 CFR § 164.530(c).
[27] 68 FR 8342, Feb. 20, 2003.
[28] 45 CFR § 160.103.
[29] 45 CFR §164.500; 68 FR 8342, Feb. 20, 2003
[30] See pp 8-9, Resolution Agreement between United States Department of Health and Human Services, Office for Civil Rights and Phoenix Cardiac Surgery, P.C., April 11, 2012
[31] 67 FR 53194, Aug. 14, 2002

HIPAA compliant Authorization from an Individual before Disclosing PHI in a Testimonial[32] and having a HIPAA compliant Business Associate Agreement[33]

B. Technical Safeguards
Encryption or other Safeguard for PHI sent by Text Message, Email or stored on an Electronic Device[34]

C. Physical Safeguards
Proper destruction of paper records containing PHI to make them unreadable by Unauthorized Persons prior to Disposal[35]

3. <u>All Privacy Rule Administrative, Technical and Physical Safeguards</u>
HHS Enforcement activities and published guidance confirm the Administrative, Technical, and Physical Safeguards required by the Privacy Rule are simply the development and implementation of Policies and Procedures reasonably designed to comply with the Standards and Implementation Specifications of the Privacy Rule, Breach Notification Rule and Security Rule.[36]
Accordingly, the Administrative, Technical and Physical Safeguards required by the Privacy Rule are the Policies and Procedures in the sections listed below.
Section 2, Basic HIPAA Policies
Section 3, Risk Analysis
Section 4, Privacy Rule
Section 5, Security Rule
Section 6, Breach Notification Rule
Section 7, Business Associates

VI. Relationship of the Privacy Rule to the Security Rule and Breach Notification Rule

Privacy Rule protection of PHI is the subject of both the Security Rule and Breach Notification Rule which address specific parts of the same topic – Uses and Disclosures of PHI not permitted by the Privacy Rule.

1. <u>The Security Rule</u>:[37]
   A. Protects PHI in Electronic form (Electronic Protected Health Information – EPHI)[38] against Uses and Disclosures not permitted by the Privacy Rule;[39] and
   B. Applies in full to Covered Entities and Business Associates.[40]
2. <u>The Breach Notification Rule</u>:[41]
   A. Defines a Breach of Unsecured PHI as the Acquisition, Access, Use, or Disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the Security or Privacy of the PHI;[42]
   B. Applies to Covered Entities and Business Associates;[43] and
   C. Specifies actions a Covered Entity and Business Associate must take:

[32] Resolution Agreement between United States Department of Health and Human Services, Office for Civil Rights and Complete P.T., Pool & Land Physical Therapy, Inc., February 2, 2016
[33] Resolution Agreement between United States Department of Health and Human Services, Office for Civil Rights and North Memorial Health Care, March 16, 2016; Resolution Agreement between United States Department of Health and Human Services, Office for Civil Rights and Triple-S Management Corporation, November 30, 2015
[34] Resolution Agreement between United States Department of Health and Human Services, Office for Civil Rights and Phoenix Cardiac Surgery, P.C., April 11, 2012; 78 FR 5634, Jan. 25, 2013
[35] Resolution Agreement between United States Department of Health and Human Services, Office for Civil Rights and Cornell Prescription Pharmacy, April 22, 2015
[36] 45 CFR §164.530(i); 45 CFR §164.530(a)(1); 45 CFR §164.306(b); 45 CFR §164.308(a)(1)(i)(2)
[37] 45 CFR Part 160 and Subparts A and C of Part 164
[38] Ibid.
[39] 45 CFR § 164.306(a)(3)
[40] 45 CFR § 164.302, See Section 5, Security Rule
[41] 45 CFR §§ 164.400-414, See Section 6, Breach Notification Rule
[42] 45 CFR § 164.402
[43] 45 CFR §§ 164.400-414

1) To determine whether an Acquisition, Access, Use, or Disclosure of PHI in a manner not permitted under the Privacy Rule was not a Breach by conducting a Breach Risk Assessment by which it can demonstrate there was a Low Probability the PHI was Compromised;[44]
2) Upon discovering a Breach of Unsecured PHI;[45] and
3) To document and demonstrate either that all Notifications required by the Breach Notification Rule were made or that the Use or Disclosure did not constitute a Breach of Unsecured PHI.[46]

VII. Privacy Rule Compliance for Covered Entities

1. Covered Entities must comply with the Privacy Rule.[47]
2. Covered Entities must develop and implement Policies and Procedures that are reasonably designed to comply with the Standards and Implementation Specifications of the Privacy and Breach Notification Rules.[48]
3. Covered Entities are liable for civil penalties for their own violations of the Privacy Rule and also for violations of the Privacy Rule by a Business Associate that is an agent of the Covered Entity.[49]
4. Covered Entities are liable for criminal penalties for violations of the Privacy Rule.[50]
5. Covered Entities must keep records of Privacy Rule compliance, cooperate with investigations and compliance reviews by HHS, submit records and permit access by HHS to its Facilities, books, records, accounts, and other sources of information, including PHI required by HHS to determine if the Covered Entity has complied or is complying with the HIPAA Rules.[51]
6. Covered Entities must designate a Privacy Official[52] who is responsible for the development and implementation of the Covered Entity's Privacy Rule and Breach Notification Rule Policies and Procedures.[53]

VIII. Privacy Rule Compliance for Business Associates

1. Business Associates including Subcontractor Business Associates must comply with specific requirements of the Privacy Rule.[54]
2. Business Associates are liable for civil penalties for their own violations of the Privacy Rule and also for violations of the Privacy Rule by a Subcontractor Business Associate that is an agent of the Business Associate.[55]
3. Business Associates are liable for criminal penalties for violations of the Privacy Rule.[56]
4. Business Associates must keep records of Privacy Rule compliance, cooperate with investigations and compliance reviews by HHS, submit records and permit access by HHS to its Facilities, books, records, accounts, and other sources of information, including PHI required by HHS to determine if the Business Associate has complied or is complying with the HIPAA Rules.[57]
5. Business Associates must be thoroughly familiar with the Privacy Rule because:
   A. Business associates generally may only Use or Disclose PHI in the same manner as a Covered Entity and any Privacy Rule limitation on how a Covered Entity may Use or Disclose PHI automatically extends to Business Associates;[58]

---

[44] 45 CFR § 164.402
[45] 45 CFR §§ 164.404-412
[46] 45 CFR § 164.414
[47] 45 CFR § 164.500
[48] 45 CFR § 164.530(i)
[49] 45 CFR § 160.300, 45 CFR §160.402(c)(1), 78 FR 5577 and 78 FR 5597, Jan. 25, 2013
[50] 42 U.S.C. § 1320d-6
[51] 45 CFR § 160.310(a)(b)(c)
[52] 45 CFR § 164.530(a)(1)(i)
[53] 45 CFR § 164.530(a)(1)(i), 45 CFR §164.530 (i)(1), See HIPAA-2, Privacy Official
[54] 45 CFR § 164.500(c), 78 FR 5597, Jan. 25, 2013
[55] 45 CFR § 160.300, 45 CFR §160.402(c)(2)
[56] 42 U.S.C. § 1320d-6, 78 FR 5597, Jan. 25, 2013
[57] Ibid.
[58] 78 FR 5597, Jan. 25, 2013

B. Under terms of their Business Associate Agreement (BAA) or Other Arrangement:[59] Business Associates have direct liability for Uses and Disclosures that do not comply with the BAA:[60]
   1) Business Associates may not Use or further Disclose PHI in a manner that would violate the Privacy Rule;
   2) Business Associates must comply with the Privacy Rule if they do something governed by the Privacy Rule on behalf of a Covered Entity; and
   3) Business Associates must have and enforce Business Associate Agreements with Subcontractor Business Associates that provide "satisfactory assurances" Subcontractors will not Use or Disclose PHI in a manner that would not be permissible if done by the Business Associate and Subcontractors obtain the same "satisfactory assurances" from their Subcontractor Business Associates "…and so on, no matter how far ''down the chain'' the information flows".[61]

6. Business Associates must comply with the Breach Notification Rule.[62] Breach Notification Rule administrative requirements are set forth in the Privacy Rule.[63]
7. Business Associates that have credible evidence of a violation of the BAA by a Subcontractor Business Associate (including Privacy and Breach Notification Rule related violations) must investigate, take reasonable steps to end the violation and, if unsuccessful, terminate a BAA or Other Arrangement if feasible.[64]
8. Business Associates must identify a Security Official who is responsible for development and implementation of the Business Associate's Policies and Procedures required by the Security Rule.[65] However, the HIPAA Rules do not provide for a Business Associate's designation of an official who is fully responsible for development and implementation of the Business Associate's Breach Notification Rule or Privacy Rule Policies and Procedures.
   A. <u>Business Associate Security Official's Limited Privacy Rule Related Responsibility</u>
   The Security Rule requires Business Associates and Subcontractor Business Associates to obtain "satisfactory assurances" in writing (a BAA or Other Arrangement) that their Subcontractor Business Associates will appropriately Safeguard PHI "in the same manner" that a Covered Entity must obtain "satisfactory assurances" from a Business Associate including the report of a Breach of Unsecured PHI.[66] Accordingly, a Business Associate Security Official is responsible for development and implementation of reasonably designed Policies and Procedures consistent with Standards and Implementation Specifications of the Privacy and Breach Notification Rules that must be included in Business Associate Contracts or Other Arrangements with Subcontractors.[67] The Security Rule assigns a Business Associate Security Official no other Privacy Rule responsibilities.
   B. <u>Designation of a Business Associate Privacy Official not Required but Essential</u>
   A Business Associate is not required to designate a Privacy Official. The HIPAA Rules provide no direction about who is to be responsible for developing and implementing Policies and Procedures required for a Business Associate to comply with the Breach Notification and Privacy Rules. This omission is notable because HHS emphasized the importance of

---

[59] 45 CFR §164.504(e), See Section 7, Business Associates
[60] 78 FR 5597, Jan. 25, 2013
[61] 45 CFR § 164.504(e)(5), 78 FR 5601, Jan. 25, 2013
[62] 45 CFR § 164.402, 45 CFR §§ 164.410-414, See Section 6, Breach Notification Rule
[63] 45 CFR § 164.530(a)(1)(i), 45 CFR §164.530 (i)(1), See HIPAA-2, Privacy Official, Section 6, Breach Notification Rule, Section 7, Business Associates,
[64] 45 CFR § 164.504(e)(1)(ii)(iii); HITECH Act Section 13401(b), PL 111-5, Feb. 17, 2009; 78 FR 5597, Jan. 25, 2013; 65 FR 82641, Aug. 14, 2000
[65] 45 CFR § 164.308(a)(2)
[66] 45 CFR § 164.308, 45 CFR §164.314; 78 FR 5694, Jan. 25, 2013; HITECH Act Section 13401(a), PL 111-5, Feb. 17, 2009
[67] 45 CFR §164.308(b)(2); 45 CFR §164.308(b)(3); 45 CFR §164.314(a); 45 CFR §164.502(e), 45 CFR §164.504(e); 45 CFR §§ 164.400-414; 45 CFR §164.530(i); 78 FR 5694, Jan. 25, 2013; HITECH Act Section 13401(a), PL 111-5, Feb. 17, 2009

accountability for an Organization's Privacy Rule compliance reside in one designated official.

> "We believe that designation of a privacy official is essential to ensure a central point of accountability within each covered entity for privacy-related issues. The privacy official is charged with developing and implementing the policies and procedures for the covered entity, as required throughout the regulation, and for compliance with the regulation generally."[68]

The same logic holds true for organizations that are Business Associates. However, the HITECH Act that made Business Associates directly liable under the HIPAA Rules did not extend their liability for compliance to all parts of the Privacy Rule. In modifying HIPAA Rules to comply with HITECH, HHS noted that while HITECH made Business Associates directly liable for Civil Money Penalties under the Privacy Rule for impermissible Uses and Disclosures of PHI and liable for Breach Notification Rule requirements applicable to Covered Entities, the statute did not make them liable for other provisions of the Privacy Rule such as providing a Notice of Privacy Practices or designating a Privacy Official.[69] HHS has not yet made a rule to provide firm direction for Business Associates to create a central point of accountability – a Business Associate Privacy/Breach Notification Official – who would be responsible for developing and implementing Policies and Procedures to comply with the Business Associate's HITECH responsibilities under the Privacy and Breach Notification Rules.

C. <u>Business Associate Best Practices – HIPAA Compliance ("Privacy") Official</u>

A Business Associate and Subcontractor Business Associate should designate one or more HIPAA Compliance Officials to be its "central point of accountability" for Privacy Rule and Breach Notification Rule issues. That HIPAA Compliance Official may be called a "Privacy Official" or its Security Official may be given responsibility for Privacy and Breach Notification Rule issues.[70] However, the title is not important. The important thing is for the Business Associate to designate a "central point of accountability" for development and implementation of its Privacy and Breach Notification Rule Policies and Procedures.

D. <u>Report – Business Associate Compliance with HIPAA</u>

The California HealthCare Foundation commissioned a survey of Covered Entity concerns about Business Associate HIPAA compliance and common Business Associate HIPAA compliance issues. [71] The report found:

1) Many Business Associates that are aware of their HIPAA compliance responsibilities have a specific person, often called the "Compliance Officer" or "Privacy Officer" who is responsible for HIPAA compliance;[72]
2) Covered Entities consider the absence of person dedicated to Business Associate HIPAA compliance is an early, "often alarming" indication of a lack of sophistication about HIPAA;[73] and
3) Business Associates worry that small Covered Entities and Subcontractor Business Associates are not prepared to comply with HIPAA.

IX. Privacy Rule Due Diligence – Covered Entities and Business Associates

1. <u>Liability for HIPAA Violations by Business Associates and Subcontractors</u>

[68] 65 FR 82744-5, Dec. 28, 2000

[69] 78 FR 5601, Jan. 25, 2013

[70] See Section 2, Basic HIPAA Policies Introduction, HIPAA-2, Privacy Official and HIPAA-3, Security Official

[71] Business Associate Compliance with HIPAA: Findings from a Survey of Covered Entities and Business Associates, October, 2014, authors: McGraw, Deven (subsequently appointed Deputy Director for Health Information Privacy, Office for Civil Rights, HHS to lead policy, enforcement and outreach efforts related to the HIPAA Privacy, Security, and Breach Notification Rules in June, 2015); Ingargiola, Susan; Wallis, Kier; Manatt, Phelps & Phillips, LLP. Funded by $500,000 received from settlement of class action lawsuit based on Breach of Unsecured PHI by Business Associate: <u>Springer v. Stanford Hospital and Clinics</u>, Cal. Super. Ct., No. BC470522, Settlement filed March 13, 2014

[72] Ibid., p. 4

[73] Ibid.

A. To ensure an Individual's PHI remains protected by all parties that create, receive, maintain, or transmit the PHI Covered Entities must obtain satisfactory assurances in writing (Business Associate Agreement or Other Arrangement) as specified by the Privacy Rule from their Business Associates, and Business Associates must do the same with regard to Subcontractors, and so on, no matter how far ''down the chain'' the PHI flows.[74] In 2016 HHS took strong action against a Covered Entity including payment of $1,550,000 and a strict Corrective Action Plan following a Breach of Unsecured PHI by the Covered Entity's Business Associate.[75]

B. A Covered Entity is liable for a HIPAA violation of a Business Associate that is its agent.[76]

C. A Business Associate is liable for a HIPAA violation of a Subcontractor Business Associate that is its agent.[77]

2. Enforcement Rule Considerations

A. Civil Money Penalties for HIPAA violations are organized in four tiers and the severity of the penalty in each tier is connected to the extent of non-compliance.[78] Tiers 3 and 4, the most severe, are for violations due to "Willful Neglect" which means the conscious, intentional failure or reckless indifference to the obligation to comply with a HIPAA Rule.[79]

B. Disclosing PHI to a Business Associate or Subcontractor Business Associate or permitting the Business Associate or Subcontractor Business Associate to create, receive, maintain or transmit PHI on its behalf without performing a Due Diligence inquiry concerning HIPAA compliance seems very likely to be a practice amounting to Willful Neglect that would expose a Covered Entity or Business Associate to the highest tiers of Civil Money Penalties.

3. Due Diligence

A. To reduce exposure under the Enforcement Rule (and minimize the risk of Breaches of Unsecured PHI) Covered Entities should conduct a Due Diligence inquiry of current and prospective Business Associates and Business Associates should do the same with current and prospective Subcontractor Business Associates.

B. The scope of a Due Diligence inquiry should be based on the circumstances of the parties. In some cases detailed inquiries may be appropriate for quality assurance or risk management and may be conducted by an expert third party auditor. However, detailed Due Diligence may carry unforeseen risk. For example:

1) Examination of a current or prospective Business Associate's HIPAA Compliance Program, Policies, Procedures and Risk Analysis by an inexperienced Person or a superficial examination may result in documented approval of an inadequate HIPAA Compliance Program that may increase exposure and liability later if the Business Associate commits a violation or suffers a Breach; and

2) Instructions intended to correct compliance deficiencies of current Business Associates may be considered the type of control direct performance of the Business Associate after the relationship was established that makes the Business Associate an agent under the Federal Common Law of Agency.[80]

C. Covered Entities and Business Associates should conduct Due Diligence Inquiries on a regular basis.[81]

---

[74] 78 FR 5573-4, Jan. 25, 2013; 45 CFR §164.502(e); 45 CFR §164.504(e)

[75] Resolution Agreement between United States Department of Health and Human Services, Office for Civil Rights and North Memorial Health Care, March 16, 2016

[76] 45 CFR § 160.402(c)(1)

[77] 45 CFR § 160.402(c)(2)

[78] 45 CFR § 160.404

[79] 45 CFR § 160.401

[80] 78 FR 5581, Jan. 25, 2013; See Section 7 – Introduction to Business Associates, Form BA-1.G, Providing More Control Over a BA – Issue of Agency and Form BA-1.B, Business Associate Due Diligence for more detailed explanation.

[81] Ibid.

D. Covered Entities should not Disclose PHI to a Business Associate or permit the Business Associate to create, receive, maintain or transmit PHI on its behalf if a Due Diligence inquiry reveals the Business Associate is not complying with HIPAA Rules.[82]
E. Business Associates should not Disclose PHI to a Subcontractor Business Associate or permit the Subcontractor Business Associate to create, receive, maintain or transmit PHI on its behalf if a Due Diligence inquiry reveals the Subcontractor Business Associate is not complying with HIPAA Rules.[83]
F. Business Associates should expect and be prepared to respond to HIPAA compliance Due Diligence inquiries from Covered Entities.[84]
G. Subcontractor Business Associates should expect and be prepared to respond to HIPAA compliance Due Diligence inquiries from Business Associates.[85]

X. The HIPAA Privacy Rule and State Health Privacy Law

1. The HIPAA Privacy Rule Generally Overrides State Health Privacy Laws

   The Privacy Rule is Federal law that overrides all State Laws relating to the Privacy of Individually Identifiable Health Information[86] with the exceptions noted below.
2. Covered Entities and Business Associates Must Comply With the HIPAA Privacy Rule – Except When State Health Privacy Law Overrides the Privacy Rule

   Covered Entities and Business Associates must comply with a State Health Privacy Law instead of the HIPAA Privacy Rule when the State Law is "More Stringent".[87]

   "More Stringent" means the State Law:[88]

   A. Prohibits or restricts a Use or Disclosure permitted by the Privacy Rule unless it imposes stricter limitations on Disclosure to the Individual or Disclosures required by HHS under the Enforcement Rule;
   B. Permits the Individual greater rights of Access or Amendment to Individually Identifiable Health Information;
   C. Provides the Individual with a greater amount of information about a Use, Disclosure, rights, and remedies concerning Individually Identifiable Health Information;
   D. Increases Privacy protections for express legal permission for Use or Disclosure of Individually Identifiable Health Information;
   E. Provides for the retention or reporting of more detailed information or for a longer duration for recordkeeping or requirements relating to Accounting of Disclosures; or
   F. Provides greater Privacy protection for the Individual who is the subject of the Individually Identifiable Health Information.
3. Include any "More Stringent" State Law in its Privacy Rule Policies and Procedures

   The HIPAA E-Tool® Privacy Rule Policies and Procedures may be easily modified to include special provisions required by State Law in consultation with Legal Counsel. Simply click

   Update to add a Special Provision.

   A table of State Health Privacy Laws HIPAA SL – State Health Privacy Law Table is located in Section 2, Basic HIPAA Policies for ready reference.
4. Multi-State Organizations

   Covered Entities and Business Associates doing business in more than one State should add any special provision to their Privacy Rule Policies and Procedures that is Required by Law of the State in which they are working.

XI. The HIPAA Privacy Rule, HIPAA Breach Notification Rule and State Breach Notification Law

---

[82] Ibid.
[83] Ibid.
[84] Ibid.
[85] Ibid.
[86] 45 CFR § 160.203
[87] 45 CFR § 160.203(b)
[88] 45 CFR § 160.202

1. The HIPAA Privacy Rule Requires Development and Implementation of HIPAA Breach Notification Rule Policies and Procedures
   Covered Entities and Business Associates must comply with the HIPAA Breach Notification Rule.[89]
2. The HIPAA Breach Notification Rule Generally Overrides State Beach Notification Law and Covered Entities and Business Associates Must Comply With the HIPAA Breach Notification Rule – Except When State Breach Notification Law Overrides the HIPAA Breach Notification Laws
   48 States, the District of Columbia, Puerto Rico, Guam and The Virgin Islands have Breach Notification Laws. The HIPAA Breach Notification Rule overrides State Breach Notification Laws except when the State Law is More Stringent.[90] For example, a State Breach Notification Law may require Individuals be notified of a Breach sooner than required by the HIPAA Breach Notification Law. And Covered Entities and Business Associates may be required to report Breaches of Unsecured PHI under both the HIPAA Breach Notification Rule and a State Breach Notification Law.
3. State Breach Notification Laws Are Not Consistent With the HIPAA Breach Notification Rule
   The timing, content and manner of reporting Breaches of Unsecured PHI differs on a State by State basis. Some States do not require notification if the Breach involved paper records or if it is determined the affected Individuals are not reasonably likely to be harmed by the Breach. The State Attorney General must be notified of a Breach in some States.
   The HIPAA E-Tool® Breach Notification Rule Policies and Procedures, required to be developed and implemented by the Privacy Rule may be easily modified to include special provisions required by State Law in consultation with Legal Counsel. Simply click
   Update to add a Special Provision.
   A table of State Breach Notification Laws BN-SL – State Breach Notification Law Table is located in Section 6, Breach Notification Rule for ready reference.

[89] 45 CFR §§ 164.400-414

[90] 45 CFR § 160.203; 78 FR 5658, Jan. 25, 2013