Security Rule Primer

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 Security Rule – Electronic Protected Health Information (EPHI)

The Security Rule[1] establishes Standards for the protection of Electronic Protected Health Information (EPHI).[2] Both Covered Entities and Business Associates must comply with the Security Rule.

EPHI

EPHI is Protected Health Information (PHI) created or received by a Covered Entity and transmitted by Electronic Media or maintained in Electronic Media.[3] By definition, all EPHI is PHI.

The Privacy Rule – Fundamental Standards for EPHI

The Privacy Rule[4] establishes:

A. Standards for Uses and Disclosures of all PHI including EPHI that Covered Entities and Business Associates are permitted and required to make;[5] and
B. Standards for the rights of Individuals regarding their own PHI including EPHI.[6]

The Privacy Rule also requires a Covered Entity to have appropriate Administrative, Technical and Physical Safeguards in place to protect the Privacy of all PHI.[7] Although the Privacy Rule was published first, HHS prepared the final Security Rule to ensure its Safeguards work "hand in glove" with Privacy Rule requirements for Administrative, Technical, and Physical Safeguards.[8]

Security Rule Administrative, Physical and Technical Safeguards

The Security Rule requires Covered Entities and Business Associates to protect against Uses and Disclosures of EPHI that are not permitted or required by the Privacy Rule.[9] To do that they must implement Security Measures consisting of appropriate Administrative, Physical and Technical Safeguards to ensure the Confidentiality, Integrity, and Security of EPHI they create, receive, maintain or transmit.[10] Accordingly, Security Rule Safeguards protecting EPHI count as Administrative, Technical and Physical Safeguards to protect the Privacy of PHI required by the Privacy Rule.

B. Protect against reasonably anticipated Threats to the Security or Integrity of EPHI;[11] and
C. Ensure compliance with the Security Rule by their Workforce.[12]

Function and Importance of the Security Rule

---

1 45 CFR Part 160 and Subparts A and C of Part 164.
2 45 CFR Part 164, Subpart C.
3 45 CFR § 160.103.
4 45 CFR Part 160 and Subparts A and E of Part 164.
5 45 CFR § 164.502(a)
6 45 CFR §§ 164.520-528.
7 45 CFR § 164.530(c)
8 67 FR 53194, Aug. 14, 2002
9 45 CFR § 164.306(a)(3).
10 45 CFR § 164.308(a)(1)(ii)(B), 45 CFR § 164.306(a), 45 CFR § 164.304.
11 45 CFR § 164.306(a)(2).
12 45 CFR § 164.306(a)(4).

Security Rule Safeguards focus on Risks that threaten EPHI – PHI maintained and transmitted Electronically. The importance of implementing those Safeguards cannot be overstated. Since the Security Rule became effective in 2005 the amount of EPHI transmitted by Electronic Media and maintained in Electronic Media with assistance from Federal financial incentives[13] has grown dramatically. However, Breaches of Unsecured EPHI that could have been prevented by Security Rule compliance are routinely reported.[14] Criminal attacks targeting EPHI are an urgent, persistent Threat. EPHI Cyber crime includes:

A. Medical Identity Theft[15]; and
B. Extortion including Ransomware attacks.[16]

BREACH PREVENTION TIP

The HIPAA Security Rule provides a Blueprint to prevent Cyber-Crime.

GUIDANCE NOTE

Flexibility of Approach

A Covered Entity or Business Associate may use any Security Measures that allow it reasonably and appropriately to implement Security Rule Standards and Implementation Specifications. In choosing Security Measures a Covered Entity or Business Associate must take into account its own specific:

1. Size, complexity, and capabilities;
2. Technical infrastructure, Hardware, and Software Security capabilities;
3. Costs of Security Measures; and
4. The probability and criticality of potential Risks to EPHI.[17]

II. Security Rule Overview

1. Security Rule Standards and Implementation Specifications
   The Security Rule is made up of Standards and Implementation Specifications. A Standard is a rule, condition, or requirement concerning the Privacy of EPHI[18] and Implementation Specifications are specific requirements or instructions for implementing a Standard.[19] Security Rule Standards and Implementation Specifications establish:
   A. Security Measures[20] – the Administrative,[21] Physical[22] and Technical Safeguards[23] to protect the Information System (interconnected EPHI resources including hardware, software, information, data, applications, communications and people)[24] of a Covered Entity or Business Associate; and
   B. Security Rule organizational requirements for Covered Entities including Business Associate Agreements, Policies, Procedures and Documentation.[25]
2. Security Rule Safeguards
   A. Security Rule Administrative Safeguards are administrative actions, and Policies and Procedures, to manage the selection, development, implementation, and maintenance of Security Measures to protect EPHI and manage the conduct of the Covered Entity's or Business Associate's Workforce in relation to the protection of EPHI.[26]

---

[13] Sec. 3011, Subtitle B, Incentives for the Use of Health Information Technology, Health Information Technology for Economic and Clinical Health Act'' or the ''HITECH Act'', Public Law 111–5—FEB. 17, 2009
[14] See, e.g. Resolution Agreements and Civil Money Penalties and Breaches Affecting 500 or More Individuals.
[15] FBI Cyber Division Private Industry Notification, PIN #: 140408-009, 8 April 2014
[16] HHS Update May 16, 2017: International Cyber Threat to Healthcare Organizations
[17] 45 CFR §164.306(b)
[18] 45 CFR §160.103
[19] Ibid.
[20] 45 CFR § 164.304
[21] 45 CFR § 164.304; 45 CFR § 164.308
[22] 45 CFR § 164.304; 45 CFR § 164.310
[23] 45 CFR § 164.304; 45 CFR § 164.312
[24] 45 CFR § 164.306
[25] 45 CFR § 164.314; 45 CFR § 316
[26] 45 CFR § 164.304

B. Security Rule Physical Safeguards are physical measures, Policies, and Procedures to protect a Covered Entity's or Business Associate's Electronic Information Systems and related buildings and equipment, from Natural and Environmental Threats, and Unauthorized intrusion.[27]

C. Security Rule Technical Safeguards are technologies, Policies, and Procedures for its use that protect and control Access to EPHI.[28]

3. Security Rule Workforce – Workforce Security Rule Awareness and Training
Workforce means employees, volunteers, trainees, and other Persons whose conduct, in the performance of work for a Covered Entity or Business Associate, is under the direct control of the Covered Entity or Business Associate whether or not they are paid by the Covered Entity or Business Associate.[29] Workforce Members who need access to PHI or EPHI to carry out their duties must receive Training on the Policies and Procedures to protect PHI and EPHI that is necessary and appropriate to carry out their duties.[30]
4. Security Rule Standards
Covered Entities and Business Associates must comply with all Security Rule Standards.[31] Implementation Specifications provide instructions for implementing most Standards. Some Standards have no Implementation Specification because the Standard itself has all necessary instructions for implementation and required compliance.
5. Security Rule Implementation Specifications – Required and Addressable
Security Rule Standards may have Implementation Specifications labeled as Required, Addressable or both.[32] (Section 5 Security Rule Policies and Procedures note whether an Implementation Specification is Required or Addressable.) The methods for complying with Required Implementation Specifications are different from methods for complying with Addressable Implementation Specifications.[33] However, in all cases, Covered Entities and Business Associates are required to comply with every Security Rule Standard, regardless of whether it has no Implementation Specification, a Required Implementation Specification, an Addressable Implementation Specification or both Required and Addressable Implementation Specifications.[34]
6. Compliance with Security Rule Required Implementation Specifications
Covered Entities and Business Associates must implement all Required Implementation Specifications.[35]
7. Compliance with Security Rule Addressable Implementation Specifications
The Security Rule's designation of an Implementation Specification as "Addressable" does not mean compliance with the Implementation Specification is "optional". To comply with an Addressable Implementation Specification Covered Entities and Business Associates must do the following things.

A. Evaluate the Addressable Implementation Specification
Covered Entities and Business Associates must evaluate each Addressable Implementation Specification to determine whether it is a reasonable and appropriate Security Measure for them to implement within their specific Security environment based on its likely contribution to protecting EPHI. The evaluation should consider a variety of factors such as

---

[27] 45 CFR § 164.304
[28] 45 CFR § 164.304
[29] 45 CFR § 160.103
[30] 45 CFR § 164.308(a)(3)(i), 45 CFR § 164.308(a)(4)(i), 45 CFR § 164.308(a)(5)(i), 45 CFR § 164.502(b), 45 CFR § 164.514(d), 45 CFR § 164.530(b)
[31] 45 CFR § 164.306(c)
[32] 45 CFR § 164.306(d)(1)
[33] 45 CFR § 164.306(d)(2); 45 CFR § 164.306(d)(3)
[34] 45 CFR § 164.306(c); 68 FR 8336, Feb. 20, 2003
[35] 45 CFR § 164.306(d)(2)

the Organization's Risk Analysis, Risk Management Program, size, complexity, capabilities and the cost of implementation.[36]

B. Implement a reasonable and appropriate Addressable Implementation Specification
If Covered Entities and Business Associates decide the Addressable Implementation Specification is reasonable and appropriate, they must implement and document the Addressable Implementation Specification.[37]

C. Implement an Alternate Security Measure to Accomplish the Same Purpose
If Covered Entities and Business Associates decide the Addressable Implementation Specification is not reasonable and appropriate in their environment but the Security Rule Standard cannot be met without implementation of an additional Safeguard, Covered Entities and Business Associates may:
1) Implement an alternate Security Measure that accomplishes the same end as the Addressable Implementation Specification found to be inappropriate; and
2) Document their decision not to implement the Addressable Implementation Specification, the rationale behind that decision, and the alternative Security Measure implemented to meet the Security Rule Standard.[38]

D. Comply with the Security Standard without implementing a Security Measure
If Covered Entities and Business Associates decide the Addressable Implementation Specification is:
1) Not reasonable or appropriate in their environment; and
2) They can meet the Security Rule Standard without implementing an alternative Security Measure in place of the Addressable Implementation Specification, Covered Entities and Business Associates must:
   a. Document the decision not to implement the Addressable Specification, the rationale behind that decision; and
   b. Document how they are meeting the Security Rule Standard.[39]

HHS provides the following example to explain how a Security Rule Standard may be met without implementing an Addressable Implementation Specification or alternative Security Measure.

> "For example, under the information access management standard, an access establishment and modification implementation specification reads: 'implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process' (45 CFR 164.308(a)(4)(ii)(c)). It is possible that a small practice, with one or more individuals equally responsible for establishing and maintaining all automated patient records, will not need to establish policies and procedures for granting access to that electronic protected health information because the access rights are equal for all of the individuals."[40]

E. Documentation
1) Covered Entities and Business Associates must create and maintain Documentation of the development and implementation of Policies and Procedures required to comply with Security Rule Standards and Implementation Specifications including Documentation of all activities associated with their evaluation and decisions with respect to Addressable Implementation Specifications.[41]
2) Covered Entities and Business Associates must keep records of Security Rule compliance, cooperate with investigations and compliance reviews by Secretary, U. S. Department of Health and Human Services (HHS), submit records and permit access by

[36] 45 CFR § 164.306(b); 45 CFR § 164.306(d)(3)(i); 68 FR 8336, Feb. 20, 2003
[37] 45 CFR § 164.306(d)(3)(ii)(A); 68 FR 8336, Feb. 20, 2003
[38] 45 CFR § 164.306(d)(3)(ii)(B)(1)(2); 68 FR 8336, Feb. 20, 2003
[39] Ibid.
[40] 68 FR 8336, Feb. 20, 2003
[41] 45 CFR § 164.316; 68 FR 8336, Feb. 20, 2003; 78 FR 5589, Jan. 25, 2013

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.[42]

III. Security Rule Standards and Implementation Specifications Covered in Section 5

Policies, Procedures and Forms in Section 5 of *The HIPAA E-Tool®* cover the majority of Security Rule Standards and Implementation Specifications with which a Covered Entity and Business Associate must comply. Some Security Rule Standards and Implementation Specifications are placed in other sections for clarity and practical use. Security Rule compliance requirements in Section 5 are grouped in four parts:

Part A – Administrative Safeguards
Part B – Physical Safeguards
Part C – Technical Safeguards
Part D – Organizational Requirements

IV. Security Rule Standards and Implementation Specifications Covered in other Sections

For clarity, access and easy use some Security Rule Standards and Implementation Specifications are grouped logically in other sections of *The HIPAA E-Tool®*. They are:

1. **Section 3, Risk Analysis – Risk Management**
   This section addresses the Security Management Process Standard and two Required Security Rule Implementation Specifications that are particularly important, Risk Analysis and Risk Management.[43] Covered Entities have been required to conduct a Risk Analysis and implement a Risk Management Program based on their Risk Analysis since 2005.[44] However, in its 2012 Pilot Audit HHS found 80% of Covered Entities still had failed to complete their Risk Analysis.[45] Risk Analysis and Risk Management became mandatory for Business Associates in 2013.[46] Section 3 provides an easy-to-use interactive, step-by-step process to perform a Risk Analysis and establish a Risk Management Program.
2. **Basic HIPAA Policies**
   HIPAA-1, HIPAA Compliance Program[47]
   HIPAA-3, Security Official[48]
3. **Section 7, Business Associates**
   Security 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 Security 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.[49] "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.[50]
   B. The content that must be covered by a BAA or Other Arrangement is specified.[51]

---

[42] 45 CFR § 160.310(a)(b)(c)
[43] 45 CFR § 164.308(a)(2)(A)(B)
[44] 45 CFR § 164.308(a)(2)(A)(B); 68 FR 8334, Feb. 20, 2003
[45] Section 8, Audit Introduction
[46] 45 CFR § 164.308(a)(2)(A)(B); 78 FR 5566, Jan. 25, 2013
[47] 45 CFR § 164.306(d)
[48] 45 CFR § 164.308(a)(2)
[49] 45 CFR § 164.308(b)(1)
[50] 45 CFR § 164.308(b)(3); 78 FR 5600-1, Jan. 25, 2013
[51] 45 CFR § 164.314(a)

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.[52] "Satisfactory assurances" obtained from a Subcontractor mean the same thing as "satisfactory assurances" obtained by a Covered Entity from a Business Associate – a BAA or Other Arrangement meeting Privacy Rule requirements.[53] 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.[54]

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."[55]

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.[56] 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.[57]

V. Security Rule Compliance for Covered Entities

1. Covered Entities must comply with the Security Rule.[58]
2. Covered Entities must develop and implement Policies and Procedures that are reasonably designed to comply with the Standards and Implementation Specifications of the Security Rule.[59]
3. Covered Entities are liable for civil penalties for their own violations of the Security Rule and also for violations of the Security Rule by a Business Associate that is an agent of the Covered Entity.[60]
4. Covered Entities are liable for criminal penalties for violations of the Security Rule.[61]
5. Covered Entities must keep records of Security Rule compliance, cooperate with investigations and compliance reviews by Secretary, U. S. Department of Health and Human Services (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.[62]
6. Covered Entities must designate a Security Official[63] who is responsible for the development and implementation of the Covered Entity's Security Rule Policies and Procedures.[64]

VI. Security Rule Compliance for Business Associates

1. Business Associates including Subcontractor Business Associates must comply with specific requirements of the Security Rule.[65]

---

[52] 45 CFR § 164.308(b)(2)
[53] 45 CFR § 164.308(b)(3)
[54] 78 FR 5601, Jan. 25, 2013
[55] 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)
[56] 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
[57] 45 CFR § 164.504(e)(3)(iii)
[58] 45 CFR § 164.302
[59] 45 CFR § 164.308(a)(1)(i)
[60] 45 CFR § 160.300, 45 CFR § 160.402(c)(1), 78 FR 5577 and 78 FR 5597, Jan. 25, 2013
[61] 42 U.S.C. § 1320d-6
[62] 45 CFR § 160.310(a)(b)(c)
[63] 45 CFR § 164.308(a)(2)
[64] 45 CFR § 164.308(a)(2); 45 CFR § 164.308(a)(1)(I);, See HIPAA-3, Security Official
[65] 45 CFR § 164.302; 78 FR 5597, Jan. 25, 2013

2. Business Associates are liable for civil penalties for their own violations of the Security Rule and also for violations of the Security Rule by a Subcontractor Business Associate that is an agent of the Covered Entity.[66]
3. Business Associates are liable for criminal penalties for violations of the Security Rule.[67]
4. Business Associates must keep records of Security Rule compliance, cooperate with investigations and compliance reviews by Secretary, U. S. Department of Health and Human Services (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.[68]
5. 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.[69]
6. 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.[70] Accordingly, The Security Rule requires a Business Associate Security Official to be 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.[71]

VII. Security Rule Due Diligence – Covered Entities and Business Associates

1. Liability for HIPAA Violations by Business Associates and Subcontractors
   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 Security 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.[72] 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.[73]
   B. A Covered Entity is liable for a HIPAA violation of a Business Associate that is its agent.[74]
   C. A Business Associate is liable for a HIPAA violation of a Subcontractor Business Associate that is its agent.[75]
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.[76] Tiers 3 and 4, the most

---

[66] 45 CFR §160.300, 45 CFR §160.402(c)(2)
[67] 42 U.S.C. § 1320d-6, 78 FR 5597, Jan. 25, 2013
[68] Ibid.
[69] 45 CFR §164.308(a)(2)
[70] 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
[71] 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
[72] 78 FR 5573-4, Jan. 25, 2013; 45 CFR §164.502(e); 45 CFR §164.504(e)
[73] Resolution Agreement between United States Department of Health and Human Services, Office for Civil Rights and North Memorial Health Care, March 16, 2016
[74] 45 CFR §160.402(c)(1)
[75] 45 CFR §160.402(c)(2)
[76] 45 CFR §160.404

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.[77]

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 their Business Associates and Business Associates should conduct a Due Diligence inquiry of their 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 inquiries may cause the Business Associate to be considered an agent under the Federal Common Law of Agency or result in inappropriate approval or ratification of the Business Associate's HIPAA compliance program.[78]
   C. Covered Entities and Business Associates should conduct Due Diligence Inquiries on a regular basis.[79]
   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.[80]
   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.[81]
   F. Business Associates should expect and be prepared to respond to HIPAA compliance Due Diligence inquiries from Covered Entities.[82]
   G. Subcontractor Business Associates should expect and be prepared to respond to HIPAA compliance Due Diligence inquiries from Business Associates.[83]

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

1. The Privacy Rule:[84]
   The Security Rule protects the same information as the Privacy Rule – the Protected Health Information (PHI) of a Covered Entity.[85] However, the Security Rule only protects that information in Electronic form.[86] Electronic PHI is simply a subset of PHI[87] and the Privacy Rule covers all PHI.[88] Accordingly, Security Rule Administrative, Physical and Technical Safeguards to protect PHI transmitted by or maintained in Electronic Media by definition are among the

[77] 45 CFR §160.401
[78] See Section 7, Business Associates and Form BA-1.B, Due Diligence Questionnaire for Business Associates
[79] Ibid.
[80] Ibid.
[81] Ibid.
[82] Ibid.
[83] Ibid.
[84] 45 CFR Part 160 and Subparts A and E of Part 164
[85] 45 CFR § 164.302
[86] 68 FR 8342, Feb. 20, 2003
[87] 45 CFR § 160.103
[88] 45 CFR § 164.500; 68 FR 8342, Feb. 20, 2003

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.[89]

2. The Breach Notification Rule:[90]
   Security Rule Addressable Implementation Specifications that EPHI be encrypted[91] provide a "safe harbor" under the Breach Notification Rule. Encrypted EPHI has been rendered unusable, unreadable, or indecipherable to Unauthorized Persons. Accordingly, it is not Unsecured PHI and Acquisition, Access, Use, or Disclosure of Encrypted EPHI in a manner not permitted by the Privacy Rule is not a Breach of Unsecured PHI that is subject to requirements of the Breach Notification Rule.[92]

IX. The Security Rule and State Health Privacy Laws

1. The Security Rule Generally Overrides State Health Privacy Laws
   The Security Rule is Federal law that overrides all State Laws relating to the Privacy of Individually Identifiable Health Information[93] with the exceptions noted below.
2. Exceptions – When State Health Privacy Law Overrides the Security Rule
   A State Law relating to the Privacy of Individually Identifiable Health Information that is More Stringent than the Security Rule must be followed.[94] More Stringent means the State Law:[95]
   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. If Applicable – Include More Stringent State Health Privacy Law in a Policy
   <<brand_title>> 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
4. Multi-State Organizations
   Covered Entities and Business Associates that operate in more than one State must be aware of State Health Privacy Laws of each State in which they operate. Security Rule Policies and Procedures for Facilities in different States should be modified as necessary upon advice by Legal Counsel to include any More Stringent State Health Privacy Law.

---

[89] 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
[90] 45 CFR §§ 164.400-414, See Section 6, Breach Notification Rule
[91] 45 CFR § 164.312(a)(2)(iv); 45 CFR § 164.312(e)(2)(ii)
[92] 45 CFR § 164.402
[93] 45 CFR § 160.201; 45 CFR § 160.203; 78 FR 5576, Jan. 25, 2013
[94] 45 CFR § 160.203(b); 78 FR 5576, Jan. 25, 2013
[95] 45 CFR § 160.202; 78 FR 5577, Jan. 25, 2013