A SUMMARY OF THE 2010 PROPOSED HIPAA REGULATIONS IMPLEMENTING HITECH

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[1] contained a provision requiring the Secretary of the Department of Health and Human Services (HHS) to publish national standards to protect the privacy and security of individually identifiable health information. These regulations, published in 2000, are known as the HIPAA Privacy Rule and the HIPAA Security Rule. In 2009, HIPAA was amended by the Health Information Technology for Economic and Clinical Health Act (HITECH), enacted as part of the American Recovery and Reinvestment Act (ARRA).[2] In July 2010, HHS released a Notice of Proposed Rulemaking (NPRM or Proposed Rule) to implement the various changes to Privacy and Security Rules required by HITECH.[3] Final regulations are expected to be published before the end of 2012.

1.) HIPAA Privacy Rule

The Privacy Rule applies to "covered health care entities" (covered entities or CEs) and their business associates. Covered entities include health plans, health care clearinghouses, and health care providers who transmit information related to certain health care transactions (such as claims and referral authorization requests) electronically.[4] The term "health plan" includes individual and group organizations that provide or pay for medical care, such as health insurance companies, health maintenance organizations (HMOs), company health plans, and government programs that pay for health care, including Medicare, Medicaid, and veterans' health care programs.[5] A health care clearinghouse is a business, such as a billing service, that processes nonstandard health information it receives from another entity into a standard format, or vice versa. [6]

a.) Individually Identifiable Health Information

The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. "Individually identifiable health information" is information that identifies or reasonably leads to identification of an individual and relates to the individual's: 1) past, present or future physical or mental health condition; 2) health care provisions; or 3) past, present, or future payment for health care

[1] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 139 (1996) (codified as amended in scattered sections of 42 U.S.C.).
[2] ARRA, Pub. L. No. 111-5, Div. A, Title XIII, § 13404, 123 Stat. 260 (2009).
[3] Modifications to the HIPAA Privacy, Security, and Enforcement Rules, 75 Fed. Reg. 40,868, 40,872-73 (proposed July 14, 2010) (to be codified at 45 C.F.R. pt. 160 and 164).
[4] HIPAA Privacy Rule, 45 C.F.R. § 160.103.
[5] 45 C.F.R. § 160.103; *see also* HHS, Summary of HIPAA Privacy Rule, http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html (last visited April 22, 2012).
[6] *Id.*

provisions. Common identifiers include name, address, birth date, or Social Security Number.[7] Individually identifiable health information subject to the Privacy Rule is "protected health information" (PHI). PHI does not include: [8] 1) a covered entity's employment records; 2) education records; or 3) certain other records subject to the Family Educational Rights and Privacy Act.[9]

b.) De-Identified Health Information

The Privacy Rule does not apply to the use or disclosure of de-identified health information.[10] Health information is considered de-identified when it no longer identifies or provides a reasonable basis to identify an individual. Information may be de-identified using either the safe harbor method or the statistical method.

To properly de-identify information in compliance with the safe harbor method, a covered entity: 1) must remove certain identifiers relating to an individual or the individual's relatives, employers, or household members; and 2) cannot have actual knowledge that the remaining information could be used to identify an individual.[11] If all of the following identifiers are removed, the information is no longer considered PHI and may be disclosed to anyone without regard to HIPAA:

- Names
- All geographic subdivisions smaller than a state, including: street, city, county, precinct, and zip code. However, the first three digits of a zip code can be used if the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people. If the unit contains less than 20,000 people, the initial digits must be changed to 000.
- All elements of dates (except year) directly related to an individual, including birth date, admission date, discharge date, and date of death. For individual over the age of 89, all dates, including the birth year, must either be removed or aggregated into a category of persons who are 90 and older.
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web universal resource locators (URLs) and Internet protocol (IP) address
- Biometric identifiers, including finger and voice prints
- Full face photos and comparable images
- Any other unique identifying number, characteristic, or code, except those permitted for re-identification purposes

---

[7] *Id.*
[8] *Id.*
[9] 20 U.S.C. §1232g.
[10] 45 C.F.R. § 164.514(a).
[11] 45 C.F.R. § 164.514(b).

Alternatively, information may be de-identified using the statistical method, in which a statistical expert applies generally accepted statistical and scientific principles to verify that an individual's identity is protected from exposure under reasonable expectations. The expert must determine that there is no more than a very small risk of having an anticipated recipient use the information, alone or in conjunction with other reasonably available information, to identify an individual.[12] HITECH requires HHS to develop further guidelines regarding de-identification; the department held a workshop to that end in March 2010.[13]

c.) Limited Data Sets

Covered entities may release limited data sets (LDS), from which certain direct patient identifiers have been removed, for research, public health, or health care operations purposes if the parties enter into a data use agreement (DUA).[14] An LDS is PHI that excludes the following identifiers of the individual or of the individual's relatives, employers, or household members:

- Names
- Postal address information except for town, city, state, and zip code
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web universal resource locators (URLs) and Internet protocol (IP) address
- Biometric identifiers, including finger and voice prints
- Full face photos and comparable images

An LDS allows covered entities to release slightly more information than de-identified data (*e.g.*, geographic information and dates), but imposes greater restrictions on how the data may be used. An LDS may only be released for certain purposes (*i.e.* research, public health, or health care operations) and requires a covered entity to enter into a DUA with the recipient of the data set.

The DUA must: 1) establish the permitted uses and disclosures of the LDS; 2) identify the individuals who may use the LDS; 3) assure that the LDS recipient will report any unlawful disclosures; require agents, including subcontractors, to agree to the same restrictions that apply to the recipient; install safeguards that prevent unlawful disclosures; and use the LDS only as permitted by the agreement or as required by law. The recipient also must agree not to re-identify the information or contact any individual whose information is part of the LDS.[15]

---

[12] *Id.*
[13] HHS.gov, Workshop on the HIPAA Privacy Rule's De-identification Standard, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/deidentificationworkshop2010.html (last visited April 27, 2012).
[14] *Id.* at § 164.514(e).
[15] *Id.* at § 164.514(e).

d.) Uses and Disclosures of PHI

The Privacy Rule defines and restricts the conditions under which a CE may use or disclose an individual's PHI. Generally, a CE is prohibited from disclosing PHI except as required or permitted by the Privacy Rule, unless the individual who is the subject of the information provides written authorization for the disclosure.[16] A CE must disclose PHI to an individual (or their personal representative) upon specific request for access to their PHI, or to the HHS Secretary when HHS conducts a compliance investigation or enforcement action.[17]

A covered entity may use and disclose PHI, without an individual's authorization, for the following purposes: 1) treatment, payment, and health care operations; 2) public interest and benefit activities; 3) incident to an otherwise permitted or required disclosure; 4) in circumstances when an individual has the opportunity to informally agree or object to disclosure of PHI or in emergency situations when the individual is incapacitated and 5) in the form of an LDS, for the purposes of research, public health, or health care operations.[18] In addition, a covered entity may use and disclose PHI pursuant to an individual's (who is the subject of the information) request or when authorized by the subject individual to disclose. The most commonly used permissive disclosures are treatment, payment, and health care operations, public interest disclosures, and as authorized by the subject individual.

e.) Treatment, Payment, and Health Care Operations (TPO)

In general, a CE may use and disclose protected health information, without authorization, for treatment, payment, and health care operation activities. Treatment includes the provision, coordination, or management of health care and related services among health care providers; consultation between providers regarding a patient; or patient referrals from one provider to another.[19] A CE may disclose PHI for its own treatment activities and the treatment activities of any another health care provider.[20] Payment includes all health plan activities associated with obtaining premiums, fulfilling coverage responsibilities, providing plan benefits, and obtaining reimbursement for furnished health care and provider activities related to payment and reimbursement.[21] A CE may use PHI for its own payment activities and may disclose PHI to another covered entity or health care provider for the payment activities of the entity receiving the information.[22]

Health care operations include a CE's administrative, financial, and quality improvement activities that are essential to maintaining the entity's business and supporting treatment and payment transactions.[23] The rule limits the definition to the following activities: 1) conducting quality assessment and improvement activities, including outcome evaluation and development of clinical guidelines, so long as generalized knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs; and case

---

[16] *Id.* at § 164.502(a).
[17] *Id.* at § 164.502(a)(2).
[18] *Id.* at § 164.502(a)(1).
[19] *Id.* at § 164.501.
[20] *Id.* at § 164.506(c)(1), (2).
[21] *Id.* at § 164.501.
[22] *Id.* at § 164.506(c)(1), (2).
[23] *Id.* at § 164.501; *see also* HHS.gov, Uses and Disclosures for Treatment, Payment, and Health Care Operations, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/usesanddisclosuresfortpo.html.

management and care coordination; 2) evaluating provider and health plan performance, reviewing the competence or qualifications of health care professionals; training to students, providers, and non-health care professionals; and activities involving accreditation, certification, and licensing; 3) specified health insurance functions, such as underwriting, premium rating, and reinsuring risk; 4) conducting or arranging for medical reviews, legal services, and audits, including fraud and abuse detection and compliance programs; 5) business planning and development; 6) business management and general administrative activities of the entity (including de-identifying protected health information and creating an LDS);[24] and 7) patient safety activities, including efforts to improve patient safety and the quality of health care delivery.[25]

A CE may disclose PHI for its own health care operations.[26] It may also disclose PHI to another CE for health care operations if the following terms are met: 1) each entity has or had a relationship with the individual who is the subject of the requested PHI; 2) the PHI pertains to that relationship; and 3) the disclosure is for one of the following purposes: conducting quality assessment and improvement activities, as described in the "health care operations" definition; evaluating provider performance, as described in the "health care operations" definition; or health care fraud and abuse detection or compliance. [27]

f.) Public Interest Activities

The Privacy Rule also permits use and disclosure of PHI, without an individual's authorization, for certain public interest purposes.[28] For example, covered entities may disclose protected health information: 1) where required by law (*e.g.*, statute, regulation, or court order);[29] 2) to a health oversight agency for activities including audits and investigations of the health care system and government benefits;[30] 3) to law enforcement officials for law enforcement purposes under certain restrictions;[31] 4) if the covered entity believes that it is necessary to prevent a serious and imminent threat to the health or safety of a person or the public and the recipient of the information is reasonably able to prevent the threat;[32] 5) for certain specialized government functions;[33] and 6) to comply with laws relating to worker's compensation or other similar programs providing benefits for work-related injuries or illness.[34]

Research is included as a public health purpose for which disclosure is permitted under limited circumstances. "Research" means any "systematic investigation, including research, development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[35] The Privacy Rule allows a covered entity to use and disclose PHI for research purposes, without an individual's authorization, in the following limited circumstances: 1) when an authorization waiver has been

---

[24] 45 C.F.R. § 164.506(3).
[25] HHS proposed this modification in its Proposed Rule on July 14, 2010. *See* Modifications to the HIPAA Privacy, Security, and Enforcement Rules, 75 Fed. Reg. at 40,914 (to be codified at 45 C.F.R. § 164.501).
[26] 45 C.F.R. § 164.506(1).
[27] *Id.* at § 164.506(4).
[28] *Id.* at § 164.512.
[29] *Id.* at § 164.512(a).
[30] *Id.* at § 164.512(d).
[31] *Id.* at § 164.512(f).
[32] *Id.* at § 164.512(j).
[33] *Id.* at § 164.512(k).
[34] *Id.* at § 164.512(l).
[35] *Id.* at § 164.501.

obtained from an Institutional Review Board or Privacy Board; 2) when a researcher represents to a covered entity that: (i) the PHI will only be used to prepare a research protocol or for similar purposes preparatory to research; (ii) no PHI will be removed from the covered entity; and (iii) the requested PHI is necessary to completing the research purposes; or 3) when the researcher: (i) represents that the use or disclosure sought is solely for research on the decedent's PHI; (ii) provides documentation of the individual's death; and (iii) represents that the requested PHI is necessary to complete the research purposes.[36] A covered entity may also use or disclose an LDS for research purposes without authorization, with a valid DUA in place.[37]

g.) Uses Requiring Individual Authorization

As noted above, a CE must obtain an individual's written authorization for any use or disclosure of PHI that is not otherwise permitted or required by the Privacy Rule.[38] A valid authorization must contain language that identifies the information to be used or disclosed; the individual's authorization to release and receive information; the purposes for disclosing the requested PHI; the expiration date or event; the individual's right to revoke the authorization; and other restrictions.[39]

h.) Marketing

A CE must obtain an individual's authorization prior to using or disclosing PHI about the individual for marketing purposes unless the use or disclosure satisfies an exception.[40] Marketing is defined as a ". . . communication about a product or service that encourages recipients of the communication to purchase or use the product or service."[41] Although this term is broad, the Privacy Rule carves out several exceptions to the authorization requirement that depend on the communication's purpose and form.[42] For example, authorization is not required for marketing communications that are made in a face-to-face conversation or in the form of a promotional gift of nominal value.[43]

In response to concerns that the health care operations exception allowed too many commercial uses and disclosures of PHI without individual authorization, the HITECH Act amended the Privacy Rule to require authorization for certain health care operations communications if the covered entity receives financial remuneration[44] for making the communication.[45] For example, consistent with the amendment, the HHS Proposed Rule would require a covered entity to obtain individual authorization for the following subsidized health care operations communications: 1) a covered entity's communications describing health-related products or services (or payment of such products or services) offered in a benefits plan, including communications about entities participating in certain

---

[36] *Id.* at § 164.512(i).
[37] *Id.* at § 164.502(a)(1).
[38] *Id.* at § 164.508.
[39] *Id.* at § 164.508(a)(3)(ii), (c)(1)-(2).
[40] 45 C.F.R. §§ 164.501, 164.514(f), 164.508(a)(4)(i); *see also* Modifications to the HIPAA Privacy, Security, and Enforcement Rules, 75 Fed. Reg. at 40,884, 40,918, 40,921-23, 40,890-91 (to be codified at 45 C.F.R. pt. 164).
[41] 45 C.F.R. § 164.501.
[42] *Id.*; 45 C.F.R. § 164.508(a)(3).
[43] 45 C.F.R. § 164.508(a)(3).
[44] HHS proposes to replace the phrase "direct or indirect payment" with "financial remuneration," which is defined as "direct or indirect payment from or on behalf of a third party whose product or service is being described." Modifications to the HIPAA Privacy, Security, and Enforcement Rules, 75 Fed. Reg. at 40,918 (to be codified at 45 C.F.R. § 164.501).
[45] ARRA, Pub. L. No. 111-5, Div. A, Title XIII, § 13406(a)(4), 123 Stat. 269-70 (2009) (codified at 42 U.S.C. 17936(a)(4)).

provider or plan networks; entities replacing or enhancing a health plan; and services or products that add value to and are not currently part of an enrollee's health plan;[46] and 2) communications for case management or care coordination, and contacting individuals about alternative treatments, to the extent these activities do not fall within the Privacy Rule's definition of treatment.[47] In addition, the NPRM imposes restrictions (beyond those listed in HITECH) for treatment-related communications made in exchange for financial remuneration, including: 1) a statement in the Notice of Privacy Practices (NPP) informing the individual that the provider may send subsidized treatment communications and 2) disclosure in the treatment communication that the communication was made in exchange for payment, along with a clear and conspicuous opportunity for the individual to elect not to receive any future subsidized communications.[48] However, providers are still allowed to make subsidized written treatment communications without authorization for purposes of care coordination or management.[49]

i.) Fundraising

Generally, the HIPAA Privacy Rule permits a covered entity to use or disclose limited PHI (only the patient's demographic information and dates of service) for fundraising purposes without individual authorization,[50] as long as the NPP informs individuals that the CE may contact them to raise funds[51] and the individual is notified that he or she may opt out of fundraising.

The HITECH Act expands on this provision and requires covered entities to provide the recipient of any fundraising communication with a clear and conspicuous opportunity to opt-out of receiving any further fundraising communications.[52] The Proposed Rule would implement this change and impose the following additional requirements: 1) the covered entity must provide an individual with an opt-out method that does not cause the individual to incur an undue burden or more than a nominal cost;[53] 2) the covered entity may not condition treatment or payment to an individual's decision of whether to receive funding raising communications;[54] and 3) the covered entity may not send fundraising communications to an individual who has elected not to receive such communications. On this last point, the current rule only requires covered entities to make "reasonable efforts" not to send fundraising communications to individuals who have opted out, but HHS intends to strengthen the policy, treating the decision to opt-out more like a revocation of authorization.[55]

j.) Sale of PHI

The HITECH Act adds a new provision to the Privacy Rule that prohibits covered entities and business associates from selling patients' PHI without authorization.[56] The authorization must expressly state that the entity is receiving remuneration in exchange for the PHI.[57]

---

[46] Modifications to the HIPAA Privacy, Security, and Enforcement Rules, 75 Fed. Reg. at 40,918 (to be codified at 45 C.F.R. § 164.501).
[47] *Id.*
[48] *Id.* at 40,923 (to be codified at 45 C.F.R. § 164.514(f)(2)).
[49] *Id.* at 40,918 (to be codified at 45 C.F.R. § 164.501).
[50] 45 C.F.R. § 164.514(f)(1).
[51] 45 C.F.R. § 164.514(f)(2).
[52] ARRA, Pub. L. No. 111-5, Div. A, Title XIII, § 13405(d)(2), 123 Stat. 264-68 (2009).
[53] Modifications to the HIPAA Privacy, Security, and Enforcement Rules, 75 Fed. Reg. at 40,922-23 (to be codified at 45 C.F.R. § 164.514(f)).
[54] *Id.*
[55] *Id.* at 40,897, 40,922-23.
[56] ARRA, Pub. L. No. 111-5, Div. A, Title XIII, § 13405(d)(2), 123 Stat. 264-68 (2009).

The following activities are exempt from this authorization requirement:

- Public Health Activities[58]
- Research[59] (covered entities and business associates may also sell PHI in LDS form for research purposes without obtaining prior authorization if the price charged reflects the cost to prepare and transmit the information.)
- Treatment and Payment[60] (Payment was not a basis for exemption originally listed in the HITECH Act, but HHS included it in the Proposed Rule and declined to impose a restriction on the amount an entity can charge for disclosing the PHI for payment purposes.)
- Health Care Operations[61]
- business associate Activities[62] (Disclosures of PHI by a covered entity to a business associate or by a business associate to a third party on behalf of the covered entity are exempted, as long as any remuneration received was for payment of activities performed by the business associate pursuant to a business associate contract.)
- Patient Requests[63] (Disclosures of PHI are exempted when a patient requests access to their medical records or an accounting of disclosures. A patient's request for an accounting of disclosures was not an exception originally listed in the HITECH Act, but HHS has decided to include it in the Proposed Rule. Under the rule, HHS would also impose a restriction on the amount of remuneration the covered entity may receive for such disclosures. A covered entity would be allowed to charge patients fees that are consistent with the rules governing the specific request.)[64]

The Proposed Rule adds the following exceptions, which were not required by the language of HITECH:

- Required by Law[65] (HHS added this new exception to ensure that covered entities continue to disclose PHI, where required by law, even if the covered entity receives remuneration for the disclosure).
- Any Other Purpose Permitted by the Privacy Rule[66] (HHS also added an exception for disclosures of PHI for any other purpose permitted by the Privacy Rule as long as the only remuneration received is a reasonable, cost-based fee to cover the cost of preparing and transmitting the PHI.)

k.) Limiting Uses and Disclosures to the Minimum Necessary

When a CE uses, discloses, or requests PHI, it must make reasonable efforts to limit such information to the "minimum necessary" needed to achieve the purpose for which the information was released or

---

[57] *Id.*
[58] Modifications to the HIPAA Privacy, Security, and Enforcement Rules, 75 Fed. Reg. at 40,891-92, 40,921 (to be codified at 45 C.F.R. § 164.508(4)(ii)(A)).
[59] *Id.* (to be codified at 45 C.F.R. § 164.508(4)(ii)(B)).
[60] *Id.* (to be codified at 45 C.F.R. § 164.508(4)(ii)(C)).
[61] *Id.* (to be codified at 45 C.F.R. § 164.508(4)(ii)(D)).
[62] *Id.* (to be codified at 45 C.F.R. § 164.508(4)(ii)(E)).
[63] *Id.* (to be codified at 45 C.F.R. § 164.508(4)(ii)(F)).
[64] *See* 45 C.F.R. § 164.524 (covered entities may only charge a reasonable, cost-based fee); 45 C.F.R. § 164.528 (covered entities may not charge a fee for an accounting of disclosures for any 12-month period).
[65] Modifications to the HIPAA Privacy, Security, and Enforcement Rules, 75 Fed. Reg. at 40,891-92, 40,921 (to be codified at C.F.R. § 164.508(4)(ii)(G)).
[66] *Id.* (to be codified at C.F.R. § 164.508(4)(ii)(H)).

requested.[67] For routine disclosures, a CE may establish standard protocols for particular types of information to limit the release to the minimum necessary.[68] For non-routine disclosures, however, a CE must conduct an individual review of each disclosure or request and develop reasonable criteria for limiting the released data to the minimum necessary.[69]

The minimum necessary standard does not apply to following situations: 1) disclosures to or requests by health care providers for treatment purposes; 2) disclosures to the individual (or personal representative) who is the subject of the information; 3) uses or disclosures made pursuant to an individual's authorization; 4) uses or disclosures to HHS for compliance review or enforcement; 5) disclosures required for compliance with HIPAA Administrative Simplification Rules; and 6) uses or disclosures that are required by law.

Although HITECH required HHS to issue guidance on what constitutes "minimum necessary," HHS did not propose any modifications or clarifications on the "minimum necessary" standard in the 2010 Proposed Rule,[70] but requested comments on what guidance is needed. In the meantime, HITECH specifies that a covered entity will be in compliance with the standard as long as, to the extent practicable, either: 1) it limits the PHI disclosed to the equivalent of an LDS or 2) if an LDS does not meet the covered entity's needs, it complies with its current compliant minimum necessary policies and procedures in disclosing a broader range of data.

l.) Business Associate Requirements

HIPAA also allows CEs to share PHI with business associates. Generally, a business associate is a person or organization, other than a member of a covered entity's workforce, performing certain functions or services on the covered entity's behalf that involve the use or disclosure of individually identifiable health information. It is possible for one CE to be the business associate of another CE.[71] The functions or activities that a business associate can perform on the CE's behalf include claims processing, data analysis, utilization review, and billing. The services that a business associate may provide for a CE are limited to legal, actuarial, accounting, consultation, data aggregation, management, administrative, accreditation, or financial services.[72]

In 2009, HITECH designated health information exchanges and other organizations that transmit PHI to a covered entity (or its business associate) and require routine access to PHI as business associates that must enter into business associate contracts with the covered entity.[73] In particular, this modification will affect Health Information Organizations (HIOs) and personal health record (PHR) vendors that transmit PHI to covered entities and require routine access.[74] In the recent Proposed Rule implementing the HITECH amendments, HHS also proposed to expand the business associate definition by adding patient safety activities to the list of functions and services a person or

---

[67] 45 C.F.R. § 164.502(b).
[68] 45 C.F.R. § 164.514(d); *see also* HHS.gov, Minimum Necessary Requirement, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.html (last visited April 27, 2012).
[69] *Id.*
[70] 45 C.F.R. § 164.504(e).
[71] 45 C.F.R. § 160.103.
[72] *Id.*
[73] ARRA, Pub. L. No. 111-5, Div. A, Title XIII, § 13408, 123 Stat. 270 (2009).
[74] HHS specifically stated that the proposed business associate definition would apply to these types of organizations. *See* Modifications to the HIPAA Privacy, Security, and Enforcement Rules, 75 Fed. Reg. at 40,912 (to be codified at 45 C.F.R. §160.103).

organization may undertake on a covered entity's behalf to give rise to a business associate relationship.[75] As such, when Patient Safety Organizations[76] conduct quality analysis with PHI, they will be treated as business associates.

Generally, a business associate is required to sign a business associate agreement (contract), comply with the HIPAA Privacy Rule and the HIPAA Security Rule, and assume other liabilities. Since HITECH, business associates are directly liable under HIPAA, which means that enforcement action can be taken against them and not just through the covered entity. HHS is also seeking to include a business associate's subcontractor in the definition of business associate.[77]

The Privacy Rule requires a CE to obtain satisfactory assurances from its business associates (in the form of a contract or other written agreement) that the business associate will appropriately safeguard any PHI it receives or creates on the covered entity's behalf.

2.) HIPAA Security Rule

a.) Entities Subject to or Affected by the Security Rule

The Security Rule applies to all covered entities, *i.e.*, health plans, health care clearinghouses, and health care providers who electronically transmit health information in connection with a covered transaction.[78] HITECH applied all of the security requirements to business associates and subcontractors of business associates.[79]

The Security Rule protects only a subset of information covered by the Privacy Rule.[80] It protects all individually identifiable health information a covered entity or business associate creates, receives, maintains or transmits in electronic form, and classifies this information as "electronic protected health information" (e-PHI). The Security Rule does not cover PHI that is transmitted or stored on paper or provided orally.

CEs and business associates of covered entities are required by the Security Rule to maintain reasonable and appropriate administrative, physical, technical, and organizational safeguards for protecting e-PHI.[81] Specifically, entities must: 1) ensure the confidentiality, integrity, and availability of all e-PHI that the covered entity creates, receives, maintains, or transmits; 2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; 3) protect against any reasonably anticipated uses or disclosures; and 4) ensure workforce compliance.

The Security Rule provides entities considerable flexibility in meeting such requirements. Entities may use any security measure that allows them to reasonably and appropriately implement the Rule's standards and implementation specifications. However, when deciding which security measures to use, an entity must always take into account: its size, complexity, and capabilities, including technical

---

[75] *Id.*
[76] 42 C.F.R. § 3.20 (2010) (defining patient safety activities and patient safety organizations).
[77] Modifications to the HIPAA Privacy, Security, and Enforcement Rules, 75 Fed. Reg. at 40,873.
[78] 45 C.F.R. § 164.302.
[79] ARRA, Pub. L. No. 111-5, Div. A, Title XIII, § 13401, 123 Stat. 260 (2009); Modifications to the HIPAA Privacy, Security, and Enforcement Rules, 75 Fed. Reg. at 40,881-33, 40,917-18 (to be codified at 45 C.F.R. §§ 164.306, 164.314).
[80] 45 C.F.R. § 164.304.
[81] *Id.* at § 164.306.

infrastructure, hardware, and software capabilities; the costs of security measures; and the probability and criticality of potential risks to e-PHI.[82] In addition to guidance from HHS regarding HIPAA, a CE should look to the guidance documents issued by the National Institute of Standards and Technology (NIST) to assist in properly securing electronic data in compliance with HIPAA.[83]

b.) Administrative Safeguards

The administrative safeguards provisions in the Security Rule require entities to adopt policies and procedures that appropriately manage the selection, development, implementation, and maintenance of security measures to protect e-PHI.[84] The most critical step in addressing this requirement is for entities to conduct risk analysis and risk management. Proper risk analysis and risk management detects and analyzes potential risks and vulnerabilities to the confidentiality or integrity of e-PHI, and reduces those risks to a reasonable and appropriate level.[85]

A CE also must apply appropriate sanctions against workforce members who fail to comply with its security policies and procedures.[86] To properly deter violations, a CE's workforce must understand the consequences for failing to comply. A CE must also implement procedures to regularly review information system activity records, such as audit logs, access reports, and security incident tracking reports.[87] This permits entities to determine whether any e-PHI is being inappropriately used or disclosed.

The Security Rule requires a CE to identify a security official who will be responsible for developing and implementing its security policies.[88] The CE must implement policies and procedures that authorize access to e-PHI only when such access is necessary based on the user or recipient's role.[89] Compliance with this standard should support an entity's compliance with the Privacy Rule's minimum necessary requirements.

A CE is required to ensure that all workforce members have appropriate access to e-PHI.[90] The CE must also prevent unauthorized users from obtaining access to such information by implementing security awareness and training programs for all workforce members. A CE must implement ongoing monitoring and evaluation plans, which requires periodic assessment of how well security policies and procedures meet the Security Rule requirements.[91]

---

[82] *Id.*
[83] *See, e.g.*, Nat'l Inst. Of Standards & Tech., U.S. Dep't of Commerce, NIST Special Publication 800-66, *An Introductory Resource Guide for Implementing the HIPAA Security Rule* (2008), *available at* http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf (last visited April 27, 2012).
[84] 45 C.F.R. § 164.308(a)(1).
[85] *Id.* at § 164.308(a)(1)(ii); *see also* CMS, Dep't of Health and Human Services, *Basics of Risk Analysis and Risk Management* (2007), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf (last visited April 27, 2012).
[86] 45 C.F.R. § 164.308(a)(1).
[87] *Id.* at § 164.308(a)(1).
[88] *Id.* at § 164.308(a)(2).
[89] *Id.* at § 164.308(a)(4).
[90] *Id.* at § 164.308(a)(3),(5).
[91] *Id.* at § 164.308(a)(8).

c.) Physical Safeguards

A CE must limit physical access to its electronic information systems and the facilities that store such information by only allowing access to authorized individuals or entities.[92] The CE must specify the proper functions of electronic computing devices that have access to or contain e-PHI, and restrict access of those devices to authorized users.[93] These restrictions include: 1) access controls, which are technical policies and procedures that allow only authorized persons or software programs to access e-PHI;[94] 2) audit controls, which are hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI;[95] 3) integrity controls, which are policies and procedures to protect e-PHI from improper alterations or destruction and adopt electronic measures to confirm that e-PHI has not been improperly altered or destroyed;[96] 4) authentication controls, which are procedures to confirm that persons or entities seeking access to e-PHI are who they claim to be;[97] and 5) transmission controls, which are technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic communications network.[98]

d.) Organizational Safeguards

Similar to the Privacy Rule, a business associate contract is required between a covered entity and a business associate before e-PHI is released.[99] If a covered entity knows of an activity or practice of the business associate that constitutes a material breach or violation of the contract, the covered entity must take reasonable steps to cure the breach or end the violation. If the business associate also maintains e-PHI for the covered entity, then the contract should be reviewed and amended to comply with the Security Rule requirements as well.

3.) HIPAA Enforcement

The Office for Civil Rights (OCR) within HHS is responsible for enforcing both the Privacy and Security Rules.[100] There is no private right of action for individuals whose information has been improperly used or disclosed. Instead, aggrieved individuals can file a complaint with OCR, which may enforce HIPAA on their behalf. While initial enforcement of the Privacy and Security Rules was minimal, in recent years, OCR has ramped up its enforcement efforts. This can be seen through a number of high-profile settlements.[101]

a.) HITECH Expansion & Revised Civil Penalties

---

[92] *Id.* at § 164.310(a).
[93] *Id.* at § 164.310(b)-(c).
[94] *Id.* at § 164.312(a).
[95] *Id.* at § 164.312(b).
[96] *Id.* at § 164.312(c).
[97] *Id.* at § 164.312(d).
[98] *Id.* at § 164.312(e).
[99] *Id.* at § 164.314.
[100] HIPAA Privacy and Security Rules, 45 C.F.R. pt. 160, 162, 164 (2010); Press Release, Dep't of Health & Human Services, HHS Delegates Authority for the HIPAA Security Rule to Office for Civil Rights (Aug. 3, 2009) (on file with author), *available at* http://www.hhs.gov/news/press/2009pres/08/20090803a.html (last visited April 27, 2012).
[101] McGuire Woods, Providers Beware: OCR Continues Aggressive Enforcement of the HIPAA Privacy and Security Rules. (April 18, 2012), available at: http://www.mcguirewoods.com/news-resources/item.asp?item=6601 (last accessed April 27, 2012).

HITECH expanded the enforcement responsibilities and tools of OCR and imposed enhanced penalties for covered entities and business associates who violate HIPAA. One significant change is requiring investigation and enforcement of complaints. The Proposed Rule implementing HITECH would require the Secretary to investigate any HIPAA complaint when a preliminary review of the facts indicates a possible violation due to willful neglect.[102] It would also revise the Secretary's discretion to conduct compliance reviews of covered entities and business associates, and require a review when there is a possible willful neglect violation.[103] These revisions will apply to violations of all the HIPAA Administrative Simplification Rules,[104] including the Breach Notification Rule issued on August 24, 2009 (discussed below).

As required by HITECH, HHS established four tiers of increasing penalty amounts to correspond to the levels of culpability associated with a HIPAA violation.[105]

The Secretary must consider both "the nature and extent of the violation" and "the nature and extent of the harm resulting from the violation."[106] In the Proposed Rule, HHS identifies a more specific, optional list of circumstances that the Secretary may also examine before calculating a penalty.[107] This list includes "the time period during which the violation occurred," "the number of individuals affected," and the "reputational harm" resulting from the violation.[108] Additionally, HHS would amend the phrase "prior violations" in the current rule to "indications of noncompliance" to reflect HHS policy of considering an entity's history of noncompliance with HIPAA rather than just its prior formal findings of violations.[109]

b.) Direct Business Associate Liability

Under the current HIPAA provisions, a covered entity is not liable for the unlawful acts of its business associates if there is a valid business associate agreement between the parties, the covered entity did not know about the violation, and the covered entity did not fail to act as required by HIPAA. The Proposed Rule would eliminate this exception and make covered entities directly liable for the actions of its business associates, regardless of whether the parties have signed a valid business associate agreement.[110] This exception, however, would not create liability for business associates that are independent contractors.[111] Whether a business associate is an agent of the covered entity will depend on the level of control that the covered entity has over the business associate.[112] The Proposed Rule would also add a parallel provision making business associates liable for the acts of its agents, including any workforce member or subcontractor acting within the scope of the agency.[113] With this

---

[102] Modifications to the HIPAA Privacy, Security, and Enforcement Rules, 75 Fed. Reg. at 40,917 (to be codified at 45 C.F.R. § 160.306).
[103] *Id.* (to be codified at 45 C.F.R. § 160.308).
[104] *Id.* at 40,875.
[105] ARRA, Pub. L. No. 111-5, Div. A, Title XIII, § 13410, 123 Stat. 271-76 (2009).
[106] 45 U.S.C. 1320d–5
[107] 75 Fed. Reg. at 40,880 (to be codified at 45 C.F.R. § 160.408).
[108] *Id.*
[109] *Id.* at 40,881.
[110] *Id.* at 40,914 (to be codified at C.F.R. § 160.402(c)).
[111] *Id.* at 40,880.
[112] *Id.*
[113] *Id.* at 40,879.

new provision, the principal-agent relationship will be crucial to determining civil money penalty liability for HIPAA violations.

4.) HIPAA Breach Notification Provisions and Security Guidance

a.) BREACH OF UNSECURED PHI

Another change to HIPAA made by the HITECH Act was the addition of new breach notification provisions requiring covered entities and business associates to notify affected individuals about breaches of unsecured PHI that compromise the privacy or security of the PHI. Covered entities must also provide notice of the breach to the Secretary of HHS and in certain circumstances, to the media. Business associates, however, are only required to notify covered entities within 60 days of any breaches. HHS issued an Interim Final Rule implementing these changes in August 2009.[114]

Encryption is not necessarily required under the Privacy Rule or the Security Rule; rather it is one of many forms suggested as a means to adequately protect PHI. For Security Rule purposes, whether encryption is the proper technology to protect a covered entity's PHI depends on the entity's security needs. However, for a covered entity to ensure that it is not subject to the new notice provisions under the Privacy Rule, it must encrypt its PHI.[115] PHI can also be secured by destroying it. Hard copy PHI, such as paper or film, must be destroyed or shredded such that it cannot be read or reconstructed. Electronic PHI, however, must be destroyed in accordance with specific government guidelines.[116]

---

[114] Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740 (August 24, 2009) (to be codified at 45 C.F.R. pt. 160 and 164), *available at* http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf.
[115] Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. at 42,742.
[116] Nat'l Inst. of Standards & Tech., U.S. Dep't of Commerce, NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices* (2007), *available at* http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.