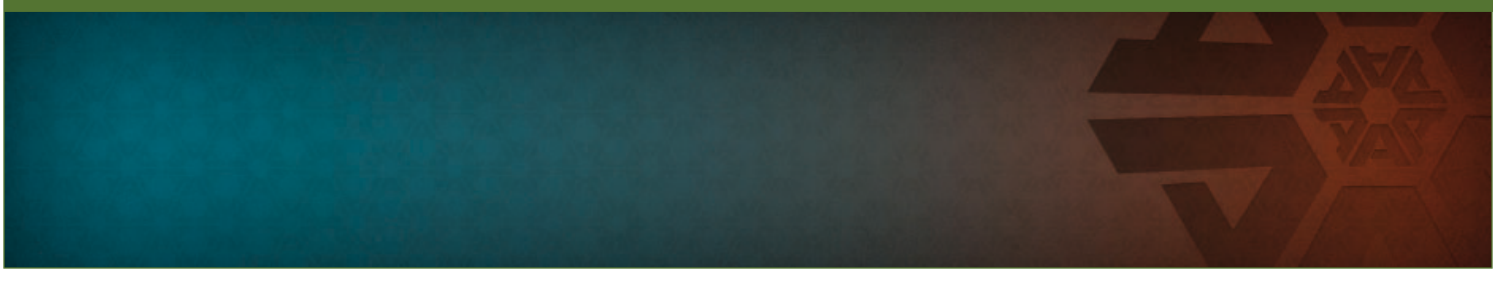
Markle Connecting for Health
Common Framework for Private and
Secure Health Information Exchange

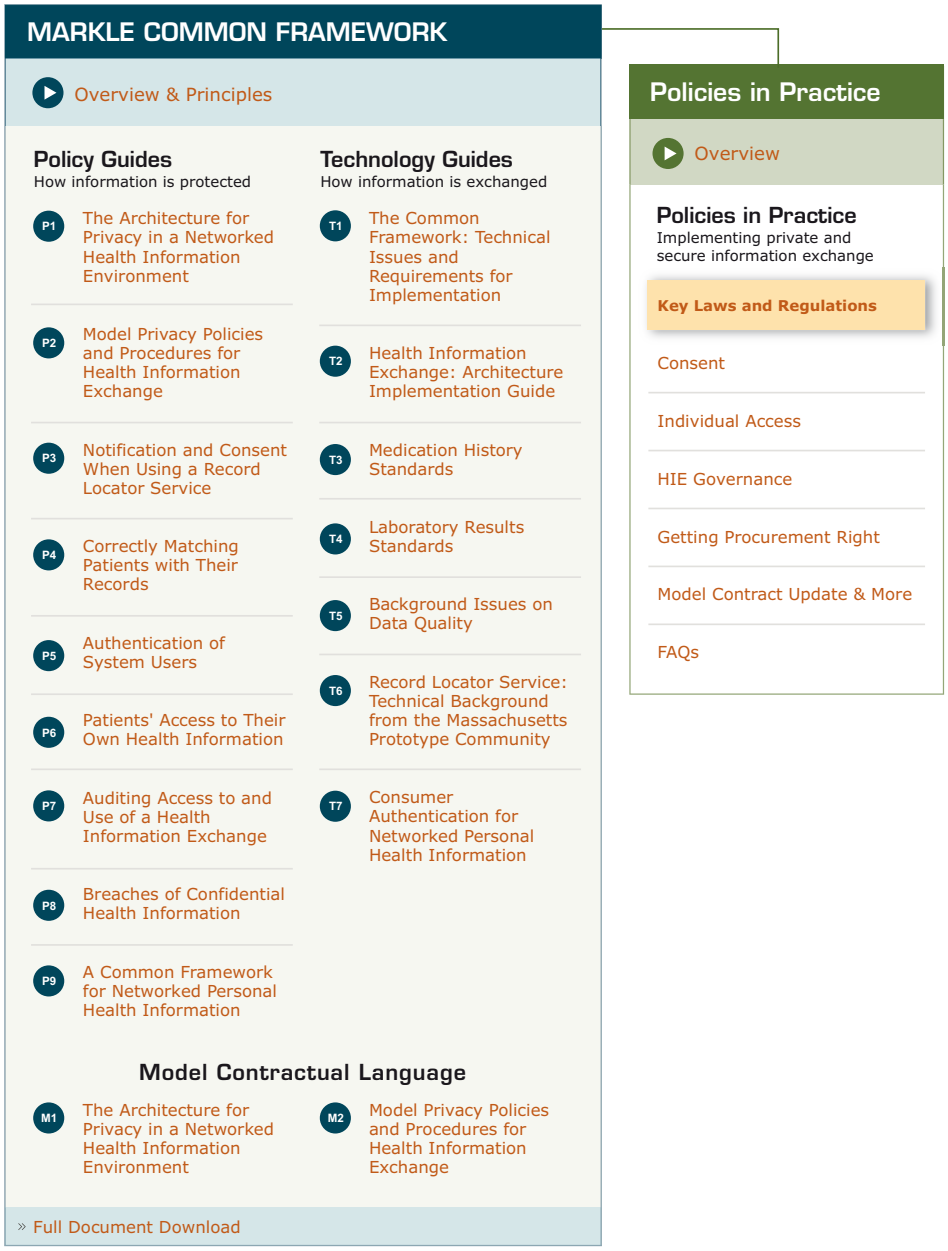
Policies in Practice

Key Laws and Regulations: Changes Relevant to the Markle Common Framework

MARKLE
CONNECTING FOR HEALTH



The document you are reading is a Markle Connecting for Health Common Framework Policies in Practice for Health Information Sharing (Policies in Practice) resource which supplements the Markle Connecting for Health Common Framework for Private and Secure Health Information Exchange (Markle Common Framework) available in its full and most current version at www.markle.org/health/markle-common-framework/connecting-professionals. The Markle Common Framework includes a set of foundational policy and technology guides published in 2006. In April 2012, a set of Policies in Practice was published to further specify these foundational documents and address a range of critical health information sharing implementation needs identified by experts working in the field.



POLICIES IN PRACTICE

Key Laws and Regulations: Changes Relevant to the Markle Common Framework

Executive Summary

The Health Information Technology for Economic and Clinical Health (HITECH) Act paves the way for an unprecedented level of federal leadership and public investment to support health information sharing efforts.[1] It also makes substantial change to the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These important changes to the HIPAA Privacy Rule (45 CFR 164, Subparts A and E) and the Security Rule (45 CFR Part 164, Subparts A and C) directly affect health information sharing efforts and their responsibilities and practices for maintaining privacy of health information. Some of these changes include:

- Giving business associates many direct statutory obligations that previously only applied to Covered Entities or to business associates by contractual obligation;
- Refining the "minimum necessary" standard;
- Increasing restrictions on the use of protected health information;
- Mandating breach notification by Covered Entities, as well as by business associates; and
- Enhancing penalties for non-compliance with HIPAA.

---

[1] The Policies in Practice apply the term "health information sharing effort" broadly to refer to any initiative that supports the electronic exchange of health information between data holders. Similar terminology includes "health information exchange (HIE)", "regional health information organization (RHIO)", and "sub-network organization (SNO)".

Markle Connecting for Health thanks Linda Malek, JD, Moses & Singer, for drafting this paper. We also thank members of the Markle Connecting for Health Health Information Exchange Advisory Committee *for their contribution in developing this paper.*

This Policies in Practice supplements the 2006 Markle Connecting for Health Common Framework for Private and Secure Health Information Exchange (Markle Common Framework) by updating relevant information on HIPAA privacy and security laws addressed throughout the Markle Common Framework. It summarizes a survey of important federal, legal and regulatory changes, since release of the Markle Common Framework through January 2012, that affect the exchange of individually identifiable health care information. Issues addressed in the Policies in Practice include:

- definition of an electronic health record
- business associates
- enforcements and penalties
- written contracts for Covered Entities
- breach notification
- marketing
- sale of protected health information
- limited data sets and minimum necessary standard,
- fundraising,
- patient's right to request nondisclosure,
- patient access to Protected Health Information, and
- accounting of disclosures

The resource does not address state laws or other types of federal laws or regulations (such as those pertaining specifically to the meaningful use of electronic health records) that may have an impact on the operations of a health information sharing effort. In addition, the resource is not intended to be used as legal advice or legal interpretation and the reader should be mindful of developments in the law when drafting and negotiating policies and contracts. It will be updated and revised from time to time to include further changes in relevant laws and regulations.

Health information sharing implementers should be mindful of state and federal laws and regulations when applying the Markle Common Framework. Implementers are encouraged to periodically refer back to this Policies in Practice for updates on new laws and regulations that are pertinent to the exchange of individually identifiable health care information.

I. Overview

Since the policies of the Markle Common Framework were released in 2006, many of the relevant privacy laws and regulations have been modified. This document is meant to assist the reader of those policies by updating the relevant information contained in policies 1 through 8 of the Policy Guides: How Information is Protected (the "Policies"), with respect to the federal privacy and security requirements. Upon its initial publication this document reflects the changes in the relevant laws and regulations since the release of the Policies through January 2012, but it will be subject to change as final laws and regulations are promulgated, and will therefore be updated and revised from time to time to include any further changes in relevant laws and regulations. It is intended to be a survey of the major federal privacy laws to date that affect the exchange of individually identifiable healthcare information, and is not intended to be used as legal advice or legal interpretation. A discussion of state law or other types of federal laws or regulations (such as those pertaining specifically to the meaningful use of electronic health records, for example) that may have an impact on the operations of an information exchange are outside the scope of this document. Because the relevant privacy laws and regulations are continually evolving, it is important that the reader be mindful of developments in the law when drafting and negotiating policies and contracts.

Enacted as part of the American Recovery and Reinvestment Act of 2009 ("ARRA"), the Health Information Technology for Economic and Clinical Health Act[2] (the "HITECH Act") has made substantial changes to the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") including the Privacy Rule (45 CFR Part 164, Subparts A and E) and the Security Rule (45 CFR Part 164, Subparts A and C)[3]. The summary below describes many of these important changes and is linked with the relevant portions of the Policies to assist the reader in updating his or her efforts to maintain privacy in a health information-sharing environment. It should be noted that while many states have laws that specifically address the collection, use, disclosure, storage and protection of health information maintained in a record, whether or not held in electronic format, neither the Policies nor this document address the application of such state laws, which are beyond the scope of the Policies and this document. The reader should endeavor to understand and implement such relevant state laws.

Some of the important changes made by the HITECH Act include making business associates subject to many obligations that previously only applied to covered entities, as that term is defined in HIPAA ("Covered Entity" or "Covered Entities"); refining the "minimum necessary" standard;

---

[2] Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 115 (February 17, 2009), codified at 42 U.S.C. §§300jj *et seq.*; §§17901 *et seq*. http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf (accessed on February 22, 2012).

[3] "Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule." *Federal Register* 75 (July 14, 2010). http://edocket.access.gpo.gov/2010/pdf/2010-16718.pdf (accessed on February 22, 2012).

increasing restrictions on the use of protected health information, as that term is defined in HIPAA ("Protected Health Information") for marketing purposes; mandating breach notification by Covered Entities as well as by business associates; and enhancing penalties for non-compliance with HIPAA.

II. Definition of Electronic Health Record

Prior to the HITECH Act there was no federal definition of an "electronic health record." Pursuant to the HITECH Act, "electronic health record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.[4] This is a very broad definition and is meant to cast a wide net applying the modified privacy and security requirements to health information that is maintained in electronic health records.

III. HIPAA Expanded to Apply Directly to Business Associates

- Application of the Security Rule to Business Associates
- Application of the Privacy Rule to Business Associates
- Application of Civil and Criminal Penalties to Business Associates
- New Obligation to Monitor Compliance of Covered Entity
- Type of Entity Considered to be a Business Associate Expanded

A. Privacy and Security Provisions of HIPAA Apply to Business Associates

Prior to the HITECH Act, the security and privacy provisions of HIPAA only extended to business associates by virtue of their business associate agreements with Covered Entities. The HITECH Act now applies many of the privacy and security regulations directly to business associates.[5]

B. Application of Security Rule to Business Associates

Under the HITECH Act, with respect to protecting Protected Health Information, both Covered Entities as well as business associates must comply with the administrative safeguards (45 C.F.R.

---

[4] HITECH Act, Section 13400(5).

[5] HITECH Act, Section 13401(a); HITECH Act, Section 13404(a).

§ 164.308), physical safeguards (45 C.F.R. § 164.310), technical safeguards (45 C.F.R. § 164.312) and the policies and procedures and documentation requirements (45 C.F.R. § 164.316) of the Security Rule.[6]

C. Application of Privacy Rule to Business Associates

The HITECH Act provides that if a business associate violates a provision of its business associate contract or any other requirement of the Privacy Rule, enforcement actions may be taken directly against the business associate.[7] Such enforcement actions are discussed further in Section IV below. Prior to the HITECH Act there was no direct enforcement action available to governmental agencies if a business associate breached its obligations regarding the privacy of Protected Health Information. Moreover, it should be noted that, as stated above, Section 13401(a) of the HITECH Act also specifically states that 45 CFR § 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), 164.312 (Technical Safeguards) and 164.316 (Policy and Procedures and documentation requirements) apply directly to a business associate of a Covered Entity in the same manner that such sections apply to the Covered Entity.

D. Application of Civil and Criminal Penalties to Business Associates

The HITECH Act applies the civil and criminal penalties of the HIPAA Security Rule directly to business associates.[8] Prior to the HITECH Act, business associates were not directly liable for such penalties. Rather, they were bound only by the contractual obligations they owed to the Covered Entities with whom they contracted.

E. New Obligation to Monitor Compliance of Covered Entity

The HITECH Act requires that if a business associate knows of a pattern of activity or practice of a Covered Entity that constitutes a material breach or violation of the Covered Entity's obligation under the business associate agreement, then the business associate is responsible to take certain actions with respect to the non-compliant Covered Entity (e.g., cure the breach, terminate the arrangement, or report to the Secretary if termination is not feasible).[9]

---

[6] Markle Connecting for Health, "P1: The Architecture for Privacy in a Networked Health Information Environment," *Markle Foundation*, last modified April 2006. http://www.markle.org/health/markle-common-framework/connecting-professionals/p1 (accessed on February 22, 2012).

[7] HITECH Act, Section 13404(a), applying to business associates all the requirements of Subchapter III (Privacy) of Chapter 156 (Health Information Technology) of Title 42 of the United States Code (The Public Health Law and Welfare).

[8] HITECH Act, Section 13401(b).

[9] HITECH Act, Section 13404(b); 45 C.F.R. § 164.504(e)(1) (ii).

F. RHIOs, HIEs and Others Deemed To Be A Business Associate

Entities that provide data transmission of Protected Health Information to a Covered Entity and require access on a routine basis to Protected Health Information, such as a Health Information Exchange Organization, a Regional Health Information Exchange, an E- prescribing Gateway, or a vendor that contracts with a Covered Entity to act on its behalf by offering a personal health record to patients as part of such Covered Entity's electronic health record, are now explicitly treated as business associates of such Covered Entity for purposes of HIPAA.[10]

IV. Enforcement and Penalties

A. Tiered Civil Monetary Penalties

The HITECH Act updated the HIPAA enforcement rule by increasing civil monetary penalties which correlate fines to the level of the violator's intent in a tiered structure, and extended such penalties to business associates. In addition to the penalties listed in the first tier, which had previously been the statutory civil monetary penalty limit, the HITECH Act added the second and third tiers of penalties:

- First tier: If the person did not know (and by exercising reasonable diligence would not have known) that a use or disclosure of Protected Health Information was in violation of a provision of HIPAA, the penalty is $100 per violation with a cap of up to $25,000 per calendar year;
- Second tier: If the violation is due to "reasonable cause"[11] but not due to willful neglect, the penalty is $1,000 per violation with a cap of up to $100,000 per calendar year;
- Third tier: If the violation was due to "willful neglect"[12] and is corrected during the 30-day period beginning on the first date the entity liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred, the penalty is $10,000 for each violation with a cap of up to $250,000 for all such violations in a calendar year;
- Fourth tier: If the violation was due to willful neglect, the maximum penalty is $50,000 per violation with a cap of up to $1,500,000 per calendar year.[13]

---

[10] HITECH Act, Section 13408.

[11] Reasonable cause means "circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated." 45 C.F.R. §160.401.

[12] Willful neglect means "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated." 45 C.F.R. § 160.401.

[13] HITECH Act, Section 13410(d)(3).

B. Enforcement for State Attorneys General

Each State Attorney General may bring a civil action on behalf of a resident of his or her state to enforce HIPAA. State Attorneys General may impose civil penalties equal to that of the "first tier" penalties as described in Section IV.A. above.[14]

C. Criminal Penalties

The HITECH Act specifically extended criminal penalties for the wrongful disclosure of individually identifiable health information under Section 1177 of the Social Security Act (42 U.S.C. Section 1320d-6) to business associates.[15] Moreover, HITECH expanded criminal liability in general. Prior to HITECH, only covered entities and certain individuals working for them could be liable directly under 42 U.S.C. Section 1320d-6.[16] Instead, individuals that were not connected with a covered entity would be prosecuted under the principles of aiding and abetting the criminal behavior.

HITECH expanded the reach of the statute by stating that any individual (whether or not connected with a covered entity) and any employee can be prosecuted directly for the violation of Section 1320d-6.[17]

V. Breach Notification

A. Mandatory Notice

The HITECH Act and the regulations promulgated pursuant to that Act created a mandatory national scheme for breach notification.

---

[14] HITECH Act, Section 13410(e)(1).

[15] HITECH Act., Section 13401(b).

[16] In a June 1, 2005 Memorandum Opinion for the General Counsel of the U.S. Department of Health and Human Services and the Senior Counsel to the Deputy Attorney General, Steven Bradbury, the Principal Deputy Assistant Attorney General, wrote: "We conclude that health plans, health care clearinghouses, those health care providers specified in the statute, and Medicare prescription drug card sponsors may be prosecuted for violations of section 1320d-6. In addition, depending on the facts of a given case, certain directors, officers, and employees of these entities may be liable directly under section 1320d-6, in accordance with general principles of corporate criminal liability, as these principles are developed in the course of particular prosecutions. Other persons may not be liable directly under this provision. The liability of persons for conduct that may not be prosecuted directly under section 1320d-6 will be determined by principles of aiding and abetting liability and of conspiracy liability." (Emphasis added.) The full memorandum is found at http://www.justice.gov/olc/hipaa_final.htm (accessed on January 27, 2012).

[17] HITECH Act, Section 13409.

B. What Constitutes a "Breach"

1. Definition

In general, the term "breach" is defined as: The acquisition, access, use or disclosure of Protected Health Information (for purposes of this Update Document only, "Unauthorized Access") that **compromises the security or privacy of Protected Health Information**.[18] "Compromises the security or privacy of Protected Health Information" is further defined to mean an Unauthorized Access that "poses a significant risk of financial, reputational, or other harm to the individual."[19] Therefore, the risk of harm must be evaluated to determine whether a "breach" has in fact occurred. This risk of harm threshold requires that a Covered Entity and business associate consider the potential harm of an Unauthorized Access of unsecured information in determining whether notification of such unauthorized access must be made.

2. Exceptions

Importantly, not all Unauthorized Access to Protected Health Information rises to the level of a "breach" as defined under the provisions of the HITECH Act. The exceptions set forth in the HITECH Act and applicable regulations include: (i) the unintentional acquisition, access, or use of Protected Health Information by a workforce member or person acting under the authority of a Covered Entity or business associate made in good faith and within the scope of authority of the Covered Entity or business associate (i.e., the workforce member or person acting on behalf of the Covered Entity or business associate),[20] provided that it does not result in further unauthorized use or disclosure;[21] (ii) an inadvertent disclosure of Protected Health Information from an authorized individual at a Covered Entity or business associate to another authorized individual at the same Covered Entity or business associate, or organized health care arrangement in which the Covered Entity participates, provided that it does not result in further unauthorized acquisition, access, use or disclosure;[22] and (iii) a disclosure of Protected Health Information where a Covered Entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.[23]

C. Risk Assessment

To determine whether such a risk of harm exists, Covered Entities and business associates are required to carry out risk assessments upon discovering an Unauthorized Access of Protected Health Information. If the Unauthorized Access of Protected Health Information meets the

---

[18] HITECH Act, Section 13400(1).

[19] 45 C.F.R. § 164.402(1).

[20] 74 Fed. Reg. 42740, 42747.

[21] HITECH Act, Section 13400(1)(A)(i); 45 C.F.R. § 164.402(2)(i).

[22] HITECH Act, Section 13400(1)(A)(ii) and (iii); 45 C.F.R. § 164.402(2)(ii).

[23] HITECH Act, Section 13400(1)(A); 45 C.F.R. § 164.402(2)(iii).

"risk of harm" threshold then the affected individuals must be given notice "without unreasonable delay" but not later than 60 days after discovery.[24] Notice to affected individuals must contain a brief description of the occurrence of the breach and the types of information that were involved in the breach, steps that individuals should take to protect themselves, how the Covered Entity is mitigating harm and contact information for individuals to ask questions and learn additional information about the breach.[25] If over 500 persons are affected in a given state, media in that state must also be notified.[26] Regulations also specify the elements that must be in the notification to the media.[27] Notice must be provided to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") "immediately" if the breach involves 500 or more individuals. If the breach is with respect to less than 500 individuals, the Covered Entity may maintain a log of any such breach occurring, and annually submit such a log to the Secretary documenting the breaches that occurred during the relevant year.[28]

D. Expanded Administrative Obligations in Connection with Breach Notification Procedures

Pursuant to the regulations promulgated under the HITECH Act for breach notification for unsecured Protected Health Information, 45 C.F.R. Parts 160 and 164,[29] the administrative requirements that Covered Entities must fulfill under the Privacy Rule have been expanded to apply in the context of the new breach notification provisions.[30]

1. Mandatory Training: Each Covered Entity is required to train all members of its workforce on policies and procedures with respect to the new breach notification provisions.[31]

2. Mandatory Training on Material Changes: In addition to requiring training for all current and new employees, the regulations specifically require training to be provided to each member of the Covered Entity's workforce whose functions are affected by a material change in the policies or procedures caused by the new breach notification provisions, within a reasonable period of time after the material change becomes effective.[32]

---

[24] HITECH Act, Section 13402(d)(1).

[25] HITECH Act, Section 13402(f); 45 C.F.R. § 164.404(c)(1).

[26] HITECH Act, Section 13402(e)(2).

[27] 45 C.F.R. § 164.406(c) (incorporating notice content requirements under § 164.404(c)).

[28] HITECH Act, Section 13402(e)(3).

[29] 74 Fed. Reg. 42470.

[30] 45 C.F.R. § 164.414(a).

[31] 45 C.F.R. § 164.530(b)(1).

[32] 45 C.F.R. § 164.530(b)(2)(c).

3. Sanctions Against Workforce Members: A Covered Entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the Covered Entity with regard to the new breach notification provisions.[33]

4. Implementation of Policies and Procedures: Covered Entities are now required to implement policies and procedures with respect to the new breach notification rules.[34]

5. Required Changes to Policies or Procedures: Covered Entities are required to change their policies and procedures as necessary and appropriate in light of the new breach notification rules.[35]

6. Process for Complaints: The Covered Entity is required to provide a process for individuals to make complaints concerning the Covered Entity's policies and procedures with respect to the new breach notification provisions.[36]

7. Protection for Individuals Who Complain: A Covered Entity cannot intimidate, threaten, coerce, discriminate against, or take any retaliatory action against any individual for the exercise of any rights established under the new breach notification requirements.[37]

8. Prohibition of Waiver: Covered Entities are prohibited from requiring individuals to waive their rights under the new breach notification provisions as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for health benefits.[38]

E. Incidental Disclosures

Under HIPAA, a Covered Entity is permitted to use or disclose Protected Health Information incident to a use or disclosure otherwise permitted or required by the Privacy Rule,[39] so long as the Covered Entity has complied with the requirements of the minimum necessary standard[40] and has implemented the requisite administrative, technical, and physical safeguards.[41] Therefore, if, for example, an improper match is returned to a requester using the Record Locator Service, then such use or disclosure is arguably incident to a use or disclosure otherwise permitted or required

---

[33] 45 C.F.R. § 164.530(e)(1).

[34] 45 C.F.R. § 164.530(i)(1).

[35] 45 C.F.R. § 164.503 (i) (2).

[36] 45 C.F.R. § 164.530(d)(1).

[37] 45 C.F.R. § 164.530(g)(1).

[38] 45 C.F.R. § 164.530(h).

[39] 45 C.F.R. § 164.502(a)(1)(iii).

[40] 45 C.F.R. § 164.502(b) and 45 C.F.R. § 164.514(d).

[41] 45 C.F.R. § 164.530(c).

by the Privacy Rule. The preamble to the breach notification rule under the HITECH Act further clarifies the concept of an incidental use or disclosure being a permitted use or disclosure under the Privacy Rule:

> "In contrast, a use or disclosure of protected health information that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule pursuant to 45 CFR 164.502(a)(1)(iii) [the incidental disclosure provision] and, therefore, would not qualify as a potential breach."[42]

Therefore, if an improper match is returned from the Record Locator Service and such use or disclosure is deemed to be an incidental use or disclosure that qualifies under 45 CFR 164.502(a)(1)(iii) then it would not be a breach under the new breach notification regulations.

If, however, a requestor obtains Protected Health Information about an individual in a way that does not qualify as an incidental use or disclosure under 45 CFR 164.502(a)(1)(iii) then the Covered Entity must conduct a risk assessment (as discussed in Section V.C. above) to determine whether a breach has occurred. Moreover, based on the particular facts and circumstances, the Covered Entity should also analyze whether one of the exceptions to unauthorized access of Protected Health Information applies (as discussed in Section V.B.2).

VI. Written Contract Extending Covered Entity's Obligations

A. Written Agreement Required

The HITECH Act requires a Covered Entity to have a written contract with all organizations that provide data transmission of Protected Health Information to the Covered Entity and require access on a routine basis to Protected Health Information, such as a Health Information Exchange Organization, a Regional Health Information Exchange, an E-prescribing Gateway, or a vendor that contracts with a Covered Entity to act on its behalf by offering a personal health record to patients as part of such Covered Entity's electronic health record.[43] Each such entity must enter into a written contract to document assurances that Protected Health Information will be properly safeguarded, as well as to apply the required administrative safeguards.[44]

---

[42] 74 FR 42740, 42744

[43] HITECH Act, Section 13408.

[44] 45 C.F.R. § 164.502(e)(2).

VII. Marketing

Under the HITECH Act, Protected Health Information generally cannot be used for marketing purposes unless certain specific exceptions apply:

A. Any Communication that Promotes a Service or Product

In general, the HITECH Act clarifies that a communication (paid or unpaid) made by a Covered Entity or business associate that is about a product or service and that encourages recipients of that communication to purchase or use the product or service is not considered a healthcare operation but rather considered to be marketing, unless such communication is made (i) to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the Covered Entity making the communication; (ii) for treatment of the individual; or (iii) for case management, for care coordination for the individual or to direct or recommend alternative treatments, therapies, healthcare providers, or settings of care to the individual.[45]

B. Exceptions to the Rule

Even if one of the exceptions (i – iii) listed above were to apply, where the Covered Entity or business associate receives or has received direct or indirect payment in exchange for making a communication, such communication is still considered marketing unless one of the following exceptions apply: (1) the communication describes a drug or biologic that is currently being prescribed for the recipient of the communication and the payment is reasonable, (2) the communication is made by the Covered Entity and the Covered Entity obtains a valid authorization from the recipient with respect to the communication, or (3) the communication is made by a business associate on behalf of the Covered Entity and the communication is consistent with the written contract between such business associate to the Covered Entity.[46]

VIII. Sale of Protected Health Information

A. Sale of Protected Health Information Prohibited

Generally, the sale of Protected Health Information is prohibited under the HITECH Act unless a Covered Entity obtains a valid authorization from the individual that includes a specification of whether Protected Health Information can be further exchanged for remuneration by the entity receiving the Protected Health Information.[47]

---

[45] HITECH Act, Section 13406(a)(1); 45 C.F.R. § 164.501.

[46] HITECH Act, Section 13406(a)(2).

[47] HITECH Act, Section 13405(d)(1).

B. Certain exceptions to this rule apply

- for public health activities,
- for research if the price charged reflects the cost of preparation and transmittal of the data,
- for the treatment of the individual,
- for a health care operation related to the sale, transfer, merger or consolidation of the Covered Entity,
- for remuneration that is provided by a Covered Entity to a business associate for activities on behalf of such Covered Entity and that involves the exchange of Protected Health Information,
- to provide an individual with a copy of such individual's Protected Health Information, or
- as otherwise determined by the Secretary of the U.S. Department Health and Human Services.[48]

IX. Limited Data Sets and the Minimum Necessary Standard

Under the HITECH Act, to comply with the HIPAA Privacy Rule's "minimum necessary" requirement, Covered Entities must "to the extent practicable" limit the use, disclosure or request of Protected Health Information to a limited data set. If needed, however, the Covered Entity can, rather than utilizing a limited data set, limit the use, disclosure or request of Protected Health Information to the minimum that they deem necessary to accomplish the intended purpose.[49] Prior to the HITECH Act, Covered Entities were required to use, disclose and request the minimum necessary Protected Health Information to accomplish the intended purpose, but there were no further defining criteria for compliance with this requirement.

Under the original HIPAA Privacy Rule, use of limited data sets was not linked to compliance with the minimum necessary standard. Rather, limited data sets were previously used only for public health, research or healthcare operations. Now, under the HITECH Act, a Covered Entity must limit, to the extent practicable, the use, disclosure or request of Protected Health Information to a limited data set. Covered Entities may now have to make use of limited data sets more frequently when disclosing health records. A limited data set consists of Protected Health Information from which an extensive list of personal identifiers is removed.[50]

---

[48] HITECH Act, Section 13405(d)(2).

[49] HITECH Act, Section 13405(b).

[50] 45 C.F.R. § 164.514(e)(2).

X. Fundraising

Any written fundraising communication that is a "health care operation" must provide an opportunity for the recipient of such communication to elect not to receive any further fundraising communication.[51]

XI. Patient's Right to Request Nondisclosure

An individual has the right to request that a Covered Entity restrict the disclosure of the Protected Health Information of such individual.[52] Pursuant to the HITECH Act, a Covered Entity must honor such request if the disclosure is to a health plan for purposes of carrying out payment or health care operations and where the Protected Health Information pertains solely to a health care item or service for which the healthcare provider has been paid out-of-pocket in full.[53] Prior to this change, individuals were permitted to request a restriction on a Covered Entity's use and disclosure of Protected Health Information, but the Covered Entity was permitted discretion regarding whether to comply with such restriction.

XII. Patient Access to Protected Health Information

A. Must Provide Copy of Record

Covered Entities maintaining electronic health records are required to give individuals copies of the records in electronic form. HIPAA required Covered Entities to provide individuals with a copy of their Protected Health Information in the form or format requested, if readily producible, and if not readily producible in such form or format, in readable hard copy form.[54] The HITECH Act clarifies this obligation by requiring that a Covered Entity that utilizes or maintains an electronic health record must provide copies of Protected Health Information in electronic format to an individual (or to such individual's designees) who requests his or her information in such format.[55]

B. Charging Costs

A Covered Entity can typically charge a "reasonable, cost-based fee" that includes copy costs, postage, and the cost of preparing an explanation/summary of the Protected Health Information provided in response to an individual's request. However, the HITECH Act limits the fee

---

[51] HITECH Act, Section 13406(b).

[52] 45 C.F.R. § 164.522(a)(1)(i).

[53] HITECH Act, Section 13405(a).

[54] 45 C.F.R. § 164.524(c)(2)(i).

[55] HITECH Act, Section 13405(e)(1).

associated with the Covered Entity's provision of a copy of electronic health records. The Covered Entity may impose a fee for providing electronic information (or summary or explanation of such information) to the requesting individual, but such fee may not be greater than "the entity's labor cost in responding to the request for the copy (or summary or explanation)."[56]

XIII. Expanded Accounting of Disclosures of Protected Health Information Maintained in Electronic Format.

A. Must Account for Disclosure for Treatment, Payment and Health Care Operations

For Covered Entities that use or maintain electronic health records, the HITECH Act eliminates the Privacy Rule exception to exclude from their accounting to individuals disclosures of Protected Health Information related to treatment, payment and health care operations. Upon the effective dates set forth in the HITECH Act, Covered Entities must provide an accounting of all disclosures of Protected Health Information, including for treatment, payment and health care operations ("TPO"), if the disclosure was made "through an electronic health record" during the previous three years.[57] The effective date for Covered Entities that implemented an electronic health record system after January 1, 2009, was January 1, 2011 (or the actual date the electronic health record system was implemented), although the effective date may be extended at the Secretary's discretion to 2013.[58] The HITECH Act requires the Secretary to promulgate regulations clarifying the types of information required to be collected about such disclosures.[59] Until this guidance is issued, and the Secretary indicates whether the effective date of this provision has been extended, Covered Entities whose electronic health record systems were implemented after January 1, 2009, should provide an accounting of disclosures of Protected Health Information for TPO purposes made through an electronic health record.

B. Who Makes Accounting to Individual

Covered Entities can now either directly account for disclosures made by business associates or provide a list of business associates to be contacted for an accounting, thus shifting the burden to the business associate to report disclosures of Protected Health Information directly to the individual if such individual requests the accounting from the business associate.[60]

---

[56] HITECH Act, Section 13405(e)(2); 45 C.F.R. § 164.524(c)(4).

[57] HITECH Act, Section 13405(c)(1)(a).

[58] HITECH Act, Section 13405(c)(4)(B) and (C). For Covered Entities that implemented electronic health record systems before or on January 1, 2009, the effective date for this provision is January 1, 2014, which also can be extended by the Secretary to as late as 2016.

[59] HITECH Act, Section 13405(c)(2).

[60] HITECH Act, Section 13405(c)(3).

XIV. Effective Dates

A. Except as otherwise stated below, the HITECH Act provisions became effective twelve months after enactment, on February 17, 2010.[61]

B. Depending on when a Covered Entity acquires an electronic health record, the effective date of the new accounting regulations varies. For electronic health records acquired as of January 1, 2009, the new accounting rules apply to disclosures of Protected Health Information made from that electronic health record on and after January 1, 2014. For electronic health records acquired after January 1, 2009, the accounting rules apply to disclosures made on and after the later of January 1, 2011, or the actual date the Covered Entity acquires an electronic health record. The compliance dates may be postponed for up to two years if it is deemed necessary by the Secretary of the U.S. Department of Health and Human Services.[62]

C. The restrictions on marketing communications went into effect and apply to written communications occurring on or after February 17, 2010.[63]

D. The new fundraising rule went into effect and applies to written communications occurring on or after February 17, 2010.[64]

E. The provision requiring the Secretary to formally investigate complaints of willful neglect went into effect as of February 17, 2011.[65]

F. The tiered increase in amount of civil monetary penalties applies to violations occurring after February 17, 2009.[66]

G. The provisions regarding enforcement by state attorneys general apply to violations occurring after February 17, 2009.[67]

H. The effective date of the Interim Final Rule; Breach Notification for Unsecured Protected Health Information, 45 C.F.R. pts 160 and 164, was September 23, 2009, which was 30 days after the publication of the interim rule as required by the HITECH Act.[68] The enforcement date of the Interim Final Rule is February 22, 2010.[69]

---

[61] HITECH Act, Section 13423.

[62] HITECH Act, Section 13405(c)(4).

[63] HITECH Act, Section 13406(c).

[64] HITECH Act, Section 13406(c).

[65] HITECH Act, Section 13410(b)(1).

[66] HITECH Act, Section 13410(d)(4).

[67] HITECH Act, Section 13410(e)(3).

[68] HITECH Act, Section 13402(j).

[69] 74 Fed. Reg. 42740, 42757.

XV. Regulatory Guidance

On July 14, 2010, HHS issued a notice of proposed rulemaking to modify the HIPAA privacy, security, and enforcement rules to comply with the changes required by the Health Information Technology for Economic and Clinical Health Act.[70] These proposed rules may be used as an indication of what the final, modified regulations could require. Those proposed regulation may be found at http://www.gpo.gov/fdsys/pkg/FR-2010-07-14/pdf/2010-16718.pdf (accessed on January 27, 2012). Moreover, various governmental agencies issue guidance related to various aspects of collection, use, disclosure and/or maintenance of identifiable information, including health information. This guidance is not statutory law enacted by a legislature nor does it constitute regulations resulting from the process of a regulatory comment period, rather the guidance of a governmental agency allows the reader to understand how the agency, tasked with the interpretation of the relevant statutes and regulations, would apply the law in certain circumstances. Such guidance may also outline a best practices approach to the application of such statutes and regulations, under the purview of the governmental agency issuing the guidance.

Relevant guidance that has been issued by government agencies since the release of the Policies includes the following:

A. The Federal Trade Commission (the "FTC")

1. Protecting Consumer Information

In December 2010, the FTC issued a document entitled "Protecting Consumer Privacy in an Era of Rapid Change-A Proposed Framework for Businesses and Policymakers." This guidance applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or device. It contains several recommended principles by which such entities should protect consumer privacy. That guidance can be accessed at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (accessed on January 27, 2012). As a follow-up to its guidance regarding protection of consumer privacy, the FTC testified before Congress on July 14, 2011, outlining its enforcement, education and policy initiatives to protect consumers' privacy. The prepared statements of the FTC to the Congressional subcommittees can be found at http://www.ftc.gov/os/testimony/110714internetprivacytestimony.pdf (accessed on January 27, 2012).

2. FTC Health Breach Notification

The FTC also enforces the FTC Health Breach Notification Rule that applies to all businesses that offer or maintain personal health records. The rule implements a requirement that such entities notify individuals in the event of a security breach with respect to their health records. The FTC Health Breach Notification Rule does not apply to a HIPAA-covered entity, as such covered entity would have to report a breach under the breach notification rule promulgated by HHS. Moreover, the FTC Health Breach Notification Rule does not apply to any other entity to the extent it engages

[70] 75 Fed. Reg. 40868.

in activities as a business associate of a HIPAA-covered entity.[71] The FTC has issued guidance for such businesses at http://business.ftc.gov/privacy-and-security/health-privacy (accessed on January 27, 2012).

B. Office of Civil Rights of the U.S. Department of Health and Human Services ("OCR")

1. Risk Analysis

In July 2010, OCR issued a publication entitled "Guidance on Risk Analysis Requirements under the HIPAA Security Rule." Such guidance is meant to assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to secure electronic protected health information by analysis of the risk and vulnerability of electronic protected health information. The guidance can be accessed at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf (accessed on January 27, 2012).

2. Security Rule Guidance

Also available through OCR is a seven-part series of CMS guidance regarding the application of the Security Rule to HIPAA covered entities, "Security Rule Educational Paper Series." The series was revised after the publication of the Policies. That series may be accessed at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html (accessed on January 27, 2012).

---

[71] 16 CFR 318.1(a). In the preamble to the FTC Health Breach Notification Rule, the FTC stated that it recognizes that in many cases a business associate of a HIPAA-covered entity may also offer PHRs directly to the public and therefore would be subject to both the HHS and FTC breach notification rules. The FTC stated that it "will deem compliance with HHS requirements governing the timing, method, and content of the notice to be compliance with the corresponding FTC rule provisions" (74 Fed. Reg. 42962, 42964). In other words, an entity that is both a business associate of a HIPAA-covered entity and also offers PHRs directly to the public can follow the HHS rules with respect to timing, method and content of the notice, but must still follow all other requirements of the FTC Health Breach Notification Rule, including reporting such breach to the FTC. "Health Breach Notification Rule; Final Rule," Federal Register 74 (August 25, 2009). http://www.ftc.gov/os/2009/08/R911002hbn.pdf (accessed on February 22, 2012).

C. The Office of the National Coordinator for Health Information Technology of the U.S. Department of Health and Human Services (the "ONC")

The ONC is the principal Federal entity charged with coordination of nationwide efforts to implement and use health information technology and electronic exchange of health information. The position of National Coordinator was created in 2004, through an Executive Order, and legislatively mandated in the Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009.

The Health IT Policy Committee is a federal advisory committee that provides recommendations on health IT policy issues to the National Coordinator for consideration. The reader may wish to keep abreast of the various recommendations made by the Health IT Policy Committee to the National Coordinator, as such recommendations may then be incorporated into official guidance of HHS or even be the basis for new regulations in the area of health IT. The recommendations of the Health IT Policy Committee may be found at http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__policy_recommendations/1815 (accessed on January 27, 2012).

Acknowledgements

Markle Connecting for Health HIE Advisory Committee

Committee Members

Phyllis Albritton
Colorado Regional Health
Information Organization (past)

Hunt Blair*
Department of Vermont Health Access

Allen Briskin, JD
Pillsbury Winthrop Shaw Pittman, LLP

Jennifer Covich Bordenick
eHealth Initiative

Carol C. Diamond, MD, MPH
Markle Foundation

Joyce Dubow
AARP Office of Policy and Strategy

Vicki Estrin
C3 Consulting, LLC

Lorraine Fernandes
IBM Information Management

Linda Fischetti, RN, MS
United States Veterans Health Administration

Liza Fox-Wylie
Colorado Regional Health
Information Organization

Mark Frisse, MD, MBA, MSc
Vanderbilt Center for Better Health

Melissa Goldstein, JD
The George Washington University
Medical Center

Adrian Gropper, MD
HealthURL

Jim Hansen
Dossia Consortium

Joseph Heyman
OptumInsight

Gerry Hinkley, JD
Pillsbury Winthrop Shaw Pittman, LLP

Zachery Jiwa*
Louisiana Department of Health & Hospitals,
State of Louisiana

Ted Kremer
Greater Rochester Regional Health
Information Organization

Alice Leiter, JD
National Partnership for Women & Families

Patricia MacTaggart
The George Washington University School
of Public Health and Health Services

Linda Malek, JD
Moses & Singer, LLP

Janet Marchibroda
Health Information Technology Initiative,
Bipartisan Policy Center

Deven McGraw, JD, MPH, LLM
Health Privacy Project, Center for Democracy
& Technology

Amanda Heron Parsons,* MD
Primary Care Information Project,
NYC Department of Health & Mental Hygiene

Gina Bianco Perez, MPA
Advances in Management, Inc.

Carol Raphael, MPA
Visiting Nurse Service of New York

Carol Robinson*
Oregon Office of Health Policy & Research

Jan Root
Utah Health Information Network

Will Ross
Redwood Mednet

Scott Schumacher, PhD
IBM Information Management

Raymond Scott
Axolotl Corporation

Randy Sermons

David Sharp
Center for Health Information Technology,
Maryland Health Care Commission

Jenny Smith
Franciscan Missionaries of Our
Lady Health System

Paul Uhrig
Surescripts

Stefaan Verhulst
Markle Foundation

Marcy Wilder, JD
Hogan Lovells

Claudia Williams,* MS
Office of the National Coordinator
for Health Information Technology

Staff

Laura Bailyn, JD
Markle Foundation

Rebekah Rockwood, MPH
Markle Foundation

Jill Schulmann, MS
Markle Foundation

Sam Sheikh, MS
Markle Foundation

Sarah Stewart
C3 Consulting, LLC

Meredith Taylor, MPH
Markle Foundation

**Note: State and Federal employees participate in the Markle HIE Advisory Committee but make no endorsement.*

We thank the members of the Markle Connecting for Health HIE Advisory Committee for providing their time and expertise to the development of the Markle Connecting for Health Common Framework Policies in Practice for Health Information Sharing resources.

We particularly thank Vicki Estrin of C3 Consulting for managing this project, and the lead authors of these resources: Allen Briskin, JD, Pillsbury Winthrop Shaw Pittman, LLP; Alice Leiter, JD, National Partnership for Women and Families; Linda Malek, JD, Moses & Singer, LLP; Deven McGraw, JD, MPH, LLM, Center for Democracy & Technology; and Stefaan Verhulst, Markle Foundation.