Summary and Analysis of Final Omnibus HIPAA Rule

Jane Hyatt Thorpe, JD
Lara Cartwright-Smith, JD, MPH
Devi Mehta, JD, MPH
Elizabeth Gray, JD
Teresa Cascio, JD
Grace Im, JD

Health Information and the Law[1]
The George Washington University Department of Health Policy

February 14, 2013

Table of Contents

Introduction

The enactment of HIPAA in 1996[2] and promulgation of HIPAA Privacy, Security, and

[1] Health Information and the Law (www.HealthInfoLaw.org) is a project of the George Washington University's Hirsh Health Law and Policy Program developed with support from the Robert Wood Johnson Foundation. The website is designed to serve as a practical online resource to federal and state laws governing access, use, release, and publication of health information. Regularly updated, the site addresses the current legal and regulatory framework of health information law and changes in the legal and policy landscape impacting health information law and its implementation.

[2] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

Enforcement Rules[3] established standards for the use and disclosure of health information. Subsequent legislation required changes to those privacy and security requirements, as well as new and expanded requirements for enforcement (including penalties) and breach notification. Specifically, the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 (HITECH),[4] enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA), established legal standards and programs to foster and support the use of interoperable health information technology and health information exchange. To ensure the privacy of protected health information, HITECH modified provisions of the Social Security Act related to the HIPAA rules and required significant changes to strengthen the HIPAA Privacy, Security, and Enforcement Rules themselves. Another recently enacted statute, the Genetic Information Nondiscrimination Act of 2008 (GINA),[5] prohibits the use of genetic information by certain health plans for underwriting purposes, which required changes to the HIPAA Privacy Rule to specifically protect genetic information like other protected health information.

On January 17, 2013, the U.S. Department of Health and Human Services (HHS) released the long-awaited omnibus final rule[6] including modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules required by the HITECH Act and revisions to the HIPAA Privacy Rule as required by GINA. HHS also used its regulatory authority to make a number of other changes to make the rules consistent with other Departmental regulations.

The omnibus Final Rule includes four separate rulemakings:

1) Final rule implementing modifications to the HIPAA Privacy, Security, and Enforcement Rules as required by HITECH that was included in a proposed rule on July 14, 2010.[7]
2) Final rule implementing changes to the HIPAA Enforcement Rule as required by HITECH that was published as an interim final rule on October 30, 2009.[8]
3) Final rule implementing changes to the Breach Notification for Unsecured Protected Health Information as required by HITECH that was published as an interim final rule on August 24, 2009.[9]
4) Final rule modifying the HIPAA Privacy Rule as required by GINA that was published

[3] Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462 (December 28, 2000).
[4] American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009), Division A, Title XIII and Division B, Title IV, Health Information Technology for Economic and Clinical Health Act (HITECH Act) (codified at 42 U.S.C. § 17930, et seq).
[5] The Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. No. 110-233, 122 Stat. 881 (2008) (codified in scattered sections of 26, 29, and 42 U.S.C.).
[6] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 5566 (January 25, 2013) (to be codified at 45 CFR pts 160 and 164).
[7] Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Notice of Proposed Rulemaking, 75 Fed. Reg. 40868 (July 14, 2010).
[8] HIPAA Administrative Simplification: Enforcement; Interim Final Rule with Request for Comments, 74 Fed. Reg. 56123 (October 30, 2009).
[9] Breach Notification for Unsecured Protected Health Information; Interim Final Rule with Request for Comments, 74 Fed. Reg. 42740 (August 24, 2009).

as a proposed rule on October 7, 2009.[10]

This Final Rule does not address the HITECH accounting for disclosures requirement[11] that was addressed in a proposed rule on May 31, 2011.[12] HHS indicated that a separate final rule would be released in the future.

The Final Rule will be effective on March 26, 2013. HHS is allowing covered entities and business associates 180 days beyond the effective date to come into compliance with most of the provisions, including the modifications to the Breach Notification Rule and the GINA changes to the HIPAA Privacy Rule. However, this grace period does not apply to the HITECH breach of unsecured protected health information provisions that became effective through the Interim Final Rule on September 23, 2009.

This section-by-section analysis gives a detailed description of the changes made in the Final Rule, as well as significant comments received and HHS' response. Also available at www.healthinfolaw.com are an overview highlighting the most significant changes and a side-by-side table comparing the proposed and final rules.

[10] Interim Final Rules Prohibiting Discrimination Based on Genetic Information in Health Insurance Coverage and Group Health Plans; Interim Final Rule with Request for Comments, 74 Fed. Reg. 51698 (October 7, 2009).
[11] HITECH Act, § 13405.
[12] HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act; Notice of Proposed Rulemaking, 76 Fed. Reg. 31426 (proposed May 31, 2011) (to be codified at 45 C.F.R. Part 164).

Modifications to the Privacy Rule

45 C.F.R. § 164.500 – Applicability

Relevant Statutory Provisions

Section 13404 of HITECH Act makes specific requirements of the Privacy Act applicable to business associates, and creates direct liability for the business associates for noncompliance.[13]

Key Provisions of the Proposed Rule

The Proposed Rule provided that, where specified, the standards, requirements, and implementation of the Privacy Rule would also apply to business associates.[14]

Key Provisions of the Final Rule

Adopted as proposed. Specifically, the Final Rule makes business associates liable for Privacy Rule obligations included in their contracts or other obligations with covered entities.[15]

Summary of Relevant Comments and HHS Response

Some commenters suggested that HHS apply the Privacy Rule to all entities that handle individually identifiable information. Another commenter sought to apply all provisions of the Privacy Rule to business associates, including requirements of implementing reasonable safeguards, training employees, and designating a privacy officer.[16]

HHS responded that it can only apply the Privacy Rule to entities covered under HIPAA. Section 13404 of the HITECH Act does not create liability for business associates for noncompliance with all requirements under the Privacy Rule, but only for those uses and disclosures of protected health information that are not in accordance with the business associate agreement or the Privacy Rule. Business associates may also be directly liable for failing to disclose protected health information when appropriate, for failing to limit the disclosure of protected health information to the minimum necessary, or for failing to enter into business associate agreements with subcontractors who create or receive protected health information on their behalf.[17]

Analysis

[13] 78 Fed. Reg. at 5591; HITECH Act §13404.
[14] 78 Fed. Reg. at 5591.
[15] 78 Fed. Reg. at 5591.
[16] 78 Fed. Reg. at 5591.
[17] 78 Fed. Reg. at 5591-92.

The application of the Privacy Rule directly to business associates represents a significant departure from previous rulemaking. Under the Final Rule, business associates must comply with the specific provisions of the Privacy Rule regarding the uses and disclosures of protected health information that are not in accordance with the business associate agreement or the Privacy Rule.

45 C.F.R. § 164.501(a) - Definition of "Health Care Operations"

Relevant Statutory Provisions

PSQIA states that Patient Safety Organizations (PSOs) are to be treated as business associates of covered health providers. Further, PSQIA states that patient safety activities of PSOs are to be treated as health care operations of covered health providers under the Privacy Rule.[18]

Key Provisions of the Proposed Rule

HHS proposed to amend the definition of "health care operations" to expressly include patient safety activities as defined by PSQIA.[19]

Key Provisions of the Final Rule

Adopted as proposed.[20]

Summary of Relevant Comments and HHS Response

Comments were generally supportive of including patient safety activities within the definition of "health care operations." [21]

Analysis

The express inclusion of PSOs under health care operations in the Privacy Rule is made final in order to conform to the definition of health care operations in the PSQIA. The final modification referencing patient safety activities clearly establishes the intersection between the Privacy Rule and the PSQIA.[22]

45 C.F.R. § 164.501(b) - Definition of Marketing

Relevant Statutory Provisions

[18] PSQIA, 42 U.S.C. § 299b-22(i); 42 C.F.R. § 3.20.
[19] 78 Fed. Reg. at 5592.
[20] 78 Fed. Reg. at 5592.
[21] 78 Fed. Reg. at 5592.
[22] 78 Fed. Reg. at 5592.

The HITECH Act limits certain health-related communications from being included under health care operations, and therefore exempt from the definition of "marketing," where a covered entity has received direct or indirect payments in exchange for making the communication.[23] If the covered entity receives such payment, the HITECH Act requires that the covered entity obtain the individual's valid authorization before making the communication or prior to the business associate making the communication.[24] The HITECH Act also provides an exception to the payment limitation that requires that the payment to the covered entity, regarding a communication describing a drug or biologic taken by the person, be reasonable in amount.[25]

Key Provisions of the Proposed Rule

HHS proposed to maintain the general definition of marketing as, "mak[ing] a communication about a product or service that encourages recipients of the communication to purchase or use the product or service."[26] In addition, the Proposed Rule included three exceptions to the marketing definition.[27]

These exceptions were: (1) health care communications, such as health-related products or services included in the plan benefits, case management or care coordination communications, or treatment related communications, except where the covered entity receives financial remuneration for making the communication;[28] (2) communications regarding a prescription drug, provided that the financial remuneration received by the covered entity is "reasonably related" to the covered entity's cost of making the communication;[29] (3) communications about health-related products and services by a health care provider to an individual, including case management or care coordination communications to the individual or to direct or recommend therapies, providers, or settings of care, provided that the communications are in writing and financial remuneration is received in exchange for making the communication and certain notice and opt out conditions are met.[30] However, the Privacy Rule makes clear that a communication to an individual regarding a health-related product or service where the covered entity receives payment from a third party in exchange for making the communication is not a health care operation and is marketing.

Finally, HHS proposed to remove language in the definition of marketing that discusses the sale of protected health information, as this practice is no longer permissible under Section 13405(d) of the HITECH Act.[31]

Key Provisions of the Final Rule

[23] HITECH Act § 13406(a).
[24] HITECH Act § 13406(a)(2)(B) and (C).
[25] HIETCH Act § 13406(a)(2)(A).
[26] 78 Fed. Reg. at 5592; 45 C.F.R. § 164.501
[27] 78 Fed. Reg. at 5592; 45 C.F.R. § 164.501.
[28] 78 Fed. Reg. at 5592-93; HITECH Act § 13406(a).
[29] 78 Fed. Reg. at 5593; HITECH Act § 13406(a)(2)(A).
[30] 78 Fed. Reg. at 5593; HITECH Act §13406(a); 45 C.F.R. §164.514(f)(2).
[31] 78 Fed. Reg. at 5594, 5596; HITECH Act § 13405(d); 45 C.F.R. § 164.508(a)(3)(i)(A).

The Final Rule requires authorizations for all treatment and health care operations communications where covered entities receive financial remuneration for making the communications from a third party whose product or service is being marketed, except for face-to-face communications or to provide a nominal promotional gift.[32] The Final Rule also applies the prior authorization requirement to business associates who receive financial remuneration from a third party in exchange for making a communication must also get prior authorization from the individual.[33]

Due to the fact that the Final Rule treats all subsidized treatment communications as marketing communications that require authorizations, HHS does not adopt the proposed notice and opt-out requirements. When communications involve financial remuneration, the authorization requirement will provide the notice under the Final Rule.[34]

The Final Rule adopts two of three additional proposed exceptions for treatment and health care operations communications about health-related products or services.[35] The first proposed exception allows communications by a covered entity to describe a health-related product or service, related to case management or care coordination or related to treatment alternatives (but not actual treatment), provided the covered entity does not receive financial remuneration in exchange for making the communication.[36] The second proposed exception excludes communications for refill reminders or other prescription-related information provided that any financial remuneration received by the covered entity for making the communication is "reasonably related" to the covered entity's cost of making the communication.[37] These two exceptions to the definition of "marketing" are finalized. HHS declines to finalize its third proposal to exclude communications related to treatment, including communications about health-related products or services provided to an individual, case management or care coordination for an individual, or to direct or recommend alternative treatments provided certain notice and opt out conditions are met.[38]

HHS also continues to exempt two other types of communications from the marketing provisions. First, communications promoting health in general, not those promoting a particular provider, do not constitute marketing and do not require individual authorization. Second, communications about government or government sponsored programs do not fall within the scope of marketing, so a covered entity may use and disclose protected health information to communicate with individuals about eligibility for public programs, such as Medicare, Medicaid, or CHIP without requiring individual authorization.[39]

---

[32] 78 Fed. Reg. at 5595.
[33] 78 Fed. Reg. at 5595-96; HITECH Act § 13406(a)(2)(C); 45 C.F.R. § 164.504(e)(2)(i).
[34] 78 Fed. Reg. at 5596; 45 C.F.R. 164.520(b)(1)(iii).
[35] 78 Fed. Reg. at 5595; 45 C.F.R. § 164.501..
[36] 78 Fed. Reg. at 5592; 45 C.F.R. § 164.501.
[37] 78 Fed. Reg. at 5596; 45 C.F.R. § 164.501.
[38] 78 Fed. Reg. at 5596.
[39] 78 Fed. Reg. at 5597.

Summary of Relevant Comments and HHS Response

The comments were mixed on the proposed changes to the definition of "marketing." Some commenters did not want any change to the existing rule, while others supported the proposed rule's decision not to require authorizations for subsidized treatment communications. HHS responded that the definition of marketing cannot be left unchanged because doing so would be inconsistent with the HITECH Act.[40]

There was concern in the comments over how to distinguish between treatment communications and communications for health care operations purposes. HHS addresses this in the Final Rule by requiring authorizations for all subsidized communications that market a health-related product or service in order to ensure that all such communications are treated as marketing communications rather than requiring entities to have two separate policies.[41]

Regarding the subsidized treatment communications, those opposed to the opt-out requirement believed: (1) all such communications require authorizations to best protect patient privacy; (2) an opt-in method would better allow individuals to decide whether they want to receive such communications; (3) a covered entity should be allowed to make these communications without an opt-out provision because it may adversely affect the quality of care provided.[42]

The majority of comments on the opt-out provision of subsidized treatment communication did not believe that there should be a way to opt-out of the communication before receiving the first such communication. Some commenters stated that the notice of privacy practices could be one way of opting out before the first communication; however, commenters expressed concern regarding the high costs associated with modifying the notice of privacy practices. However, HHS declined to adopt the notice and opt-out provisions because subsidized treatment communications will now be treated as marketing communications that require authorization.[43]

There were a large number of comments on the exception to the definition of marketing on prescription drug communications. Most commenters were in support of the exception, while those who did not support it felt that it should be treated as treatment communication, requiring notice and opt-out. There was broad support for the cost limitation of this exception being reasonably related to the cost of the communication. HHS did make changes suggested by commenters in the Final Rule.[44]

Analysis

[40] 78 Fed. Reg. at 5595; HITECH Act § 13406(a).
[41] 78 Fed. Reg. at 5594-95.
[42] 78 Fed. Reg, at 5594.
[43] 78 Fed. Reg. at 5595; 45 C.F.R. § 164.520(b)(1)(iii).
[44] 78 Fed. Reg. at 5595-96.

Among the reasons for requiring authorizations for communications regarding both treatment and health care operations, HHS notes it would be difficult to distinguish between the two, so it will treat all as marketing communications.[45]

While HHS does not adopt the notice and opt-out provisions for subsidized treatment communications, covered entities that desire to include the notice requirement in the Notice of Privacy Practices are able to do so. The notice and opt out provisions for subsidized treatment communications are also not adopted in the Final Rule because the authorization requirement provides covered entities a more uniform system. Therefore, if a person declines to sign the authorization, he or she declines to receive subsidized treatment communications and the covered entity is prohibited from making them.[46]

The Final Rule also adopts the Proposed Rule's exception for refill or drug prescriptions. The Final Rule clarifies that the scope of this exceptions includes generic prescriptions, drug adherence communications, and communications on all aspects of a drug delivery system. The Final Rule clarifies what constitutes reasonable remuneration under the exception as that which covers "costs of labor, supplies, and postage to make the communication." If the financial remuneration generates a profit, it is prohibited.[47]

The Final Rule also clarifies a covered entity's promotion of member benefits or discounts. If a mailing house or business associate of the covered entity receives financial remuneration from the entity whose product is being promoted, this is a marketing communication where individual authorization is needed. However, if the materials being provided to promote the discount were provided by the covered entity or business associate and no payment was made by the entity relating to the mailing or distribution no authorization would be needed.[48]

45 C.F.R. 164.501(b) - Definition of Financial Remuneration

Relevant Statutory Provisions

The HITECH Act describes the limitations on permitted health care operations using the term "direct or indirect payment." However, to avoid confusion with the term "payment" used in the Privacy Rule regarding payment for health care and for consistency with the term "remuneration," used in the marketing requirement in Section 164.508(a)(3), there is a need to reconcile the terms. [49]

Key Provisions of the Proposed Rule

HHS proposed to define "financial remuneration" in the definition of marketing to mean "direct or indirect payment from or on behalf of a third party whose product or service is

[45] 78 Fed. Reg. at 5595.
[46] 78 Fed. Reg. at 5595.
[47] 78 Fed. Reg. at 5596-97.
[48] 78 Fed. Reg. at 5597.
[49] HITECH Act § 13406(a)(4); 45 C.F.R. § 164.508(a)(3).

being described." The Proposed Rule also clarified that financial remuneration does not include direct or indirect payments for the treatment of an individual, and that financial remuneration, as opposed to in-kind or any other types of remuneration, is relevant for purposes of marketing. Therefore, HHS proposed that the rule modify remuneration to "financial remuneration" for the required authorization provisions for marketing. The Proposed Rule also emphasized that the financial remuneration must be in exchange for making the communication itself and be from or on behalf of the entity whose product or service is being described.[50]

Key Provisions of the Final Rule

Adopted as proposed. The Final Rule also clarifies the differences between direct and indirect payments. HHS confirms that financial remuneration does not include non-financial benefits, but only includes payments made in exchange for making communications about a product or service. If the financial remuneration received by the covered entity is for a purpose other than for making the communication, the marketing provision does not apply.[51]

Summary of Relevant Comments and HHS Response

There was some support of the use of the term "financial remuneration," but there were some comments seeking clarification on the scope of the definition and on the meaning of "direct or indirect payments."[52] Commenters also sought clarification on whether non-financial benefits constituted financial remuneration, which HHS clarified as not being financial remuneration.[53]

Analysis

None.

45 C.F.R. § 164.502(a) and (b)- Permitted and Required Uses and Disclosures by Business Associates

Relevant Statutory Provisions

As noted above, the HITECH Act makes specific provisions of the Privacy Rule applicable to business associates, and creates direct liability for uses and disclosures of protected health information by business associates that do not comply with the business associate agreement or other arrangements. Section 13404(a) of the HITECH Act also applies the privacy requirements to business associates as if they are covered entities.[54] The HITECH Act also includes provisions that apply the Privacy Rule's provision on

[50] 78 Fed. Reg. at 5593.
[51] 78 Fed. Reg. at 5595-96.
[52] 78 Fed. Reg. at 5594-95.
[53] 78 Fed. Reg. at 5594-96.
[54] HITECH Act § 13404(a).

knowledge of a pattern of activity that constitutes material breach and HIPAA's civil and criminal penalties to business associates as well.[55]

Key Provisions of the Proposed Rule

In the Proposed Rule, HHS proposed to modify Section 164.502(a) to apply the requirement that a covered entity may not use or disclose protected health information except as permitted by the Privacy Rule or Enforcement Rule to business associates.[56]

Specifically, HHS proposed that a business associate may only use or disclose protected health information as required or allowed by its business associate agreement or other arrangement, or as required by law. Furthermore, a business associate may not use or disclose protected health information in a way that would violate the Privacy Rule if done by a covered entity, except that the business associate is permitted to use or disclose the health information for proper management and administration purposes and to provide data aggregation services to the covered entity if such uses and disclosures are permitted in the business associate agreement.[57]

The Proposed Rule also required that a business associate disclose protected health information when required by the Secretary under Subpart C of Part 160 to determine whether the business associate is in compliance with the section, or to the covered entity, individual, or individual's designee to satisfy the covered entity's obligation regarding an individual's request for an electronic copy of protected health information. Therefore, the Proposed Rule would require business associates (as already required of covered entities) who maintain electronic health records, to provide an individual or his or her designee a copy of the information in electronic format when requested.[58]

The Proposed Rule also made minor changes clarifying that the provisions in Section 164.502(a)(1) and (2) only apply to permitted and required uses and disclosures of covered entities, and to clarify that a covered entity is required to disclose any protected health information to the Secretary in order to determine compliance with all of HIPAA not just the Privacy Rule.[59]

Key Provisions of the Final Rule

Adopted as proposed. The Final Rule also clarifies that liability attaches to business associates for impermissible uses and disclosures of protected health information when a person receives, creates, maintains, or transmits protected health information on behalf of a covered entity or business associate and otherwise meets the definition of a business associate. Liability does not depend on the type of protected health information or the

[55] HITECH Act §§ 13404(b) and (c).
[56] 78 Fed. Reg. at 5597-98.
[57] 78 Fed. Reg. at 5598.
[58] 78 Fed. Reg. at 5598.
[59] 78 Fed. Reg. at 5598.

type of business associate entity, unless the entity falls within an exception of the definition of a business associate.[60]

The Final Rule also sets forth the HIPAA provisions for which a business associate can be held directly liable. According to HITECH, and under HIPAA, business associates can be held directly liable for:[61]

- Impermissible uses and disclosures;
- Failure to provide breach notification to the covered entity;
- Failure to provide access to an electronic copy of protected health information to a covered entity, an individual, or an individual's designee;
- Failure to disclose protected health information when required by the Secretary to investigate a business associate's compliance with the HIPAA rules;
- Failure to provide an accounting of disclosures; and
- Failure to comply with the provisions of the Security Rule.

Business associates are contractually liable for other requirements in the business associate agreement as discussed below. HHS also clarifies that business associates are liable for providing electronic access to protected health information in accordance with the terms in the business associate agreement, which may require that the business associate provide electronic access directly or provide the electronic health information to the covered entity.[62]

Summary of Relevant Comments and HHS Response

Several commenters expressed concern over the increased liability that business associates would face under the proposed rule. HHS responded to the concern over increased liability by noting that the direct liability for business associates is provided for in the HITECH Act. There were also comments asking for clarification for what types of uses and disclosures would trigger liability for business associates, which the Final Rule addresses, as noted above.[63]

Analysis

None.

45 C.F.R. § 164.502(b) - Minimum Necessary Standard for Business Associates

Relevant Statutory Provisions

HITECH addresses and applies the minimum necessary standard to business associates.[64]

[60] 78 Fed. Reg. at 5598; 45 C.F.R. §164.502(a)(3)-(5).
[61] 78 Fed. Reg. at 5598-99; HITECH Act § 13404; 45 C.F.R. § 164.502(a).
[62] 78 Fed. Reg. at 5599.
[63] 78 Fed. Reg. at 5598.
[64] 78 Fed. Reg. at 5599; HITECH Act §§ 13405(b), 13404(a).

Key Provisions of the Proposed Rule

In the Proposed Rule, HHS sought to require business associates to limit protected health information to the minimum necessary to accomplish the intended purpose. Under the Proposed Rule, a business associate would not be able to make a permitted use or disclosure under the Privacy Rule unless it applied the minimum necessary standard[65]

Key Provisions of the Final Rule

Adopted as proposed. HHS notes in the Final Rule that requests directed at another business associate or covered entity must also be limited to the minimum necessary. Application of the minimum necessary standard by a business associate will vary, but the business associate agreement must limit the use and disclosure of protected health information to be consistent with the minimum necessary policies.[66]

Summary of Relevant Comments and HHS Response

There was general support for applying the minimum necessary provision for use and disclosure of protected health information to business associates. There were some requests for clarification of the application of the minimum necessary standard. HHS stated that it will issue future guidance on business associates' application of the minimum necessary standard.[67]

Analysis

None.

45 C.F.R. §§ 164.502(e) and 164.504(e) - Business Associate Agreements

Relevant Statutory Provisions

HHS is using its regulatory authority through the HITECH Act to issue rules regarding a covered entity and business associate's new obligations under the law concerning satisfactory assurances in the form of a written contract or arrangement.[68]

Key Provisions of the Proposed Rule

The Proposed Rule paralleled the existing rule, allowing a business associate to disclose protected health information to a business associate that is a subcontractor and allowing the subcontractor to create or receive protected health information on its behalf if the

[65] 78 Fed. Reg. at 5599; 45 C.F.R. § 164.502(b).
[66] 78 Fed. Reg. at 5599.
[67] 78 Fed. Reg. at 5599.
[68] 78 Fed. Reg. at 5599-60; HITECH Act § 13404.

business associate received assurances that the subcontractor would appropriately safeguard the information. The proposed rule also clarified that the covered entity was not responsible for obtaining the assurances from the subcontractor, but that it was the responsibility of the business associate to do so.[69]

HHS also proposed modifications to Section 164.502(e)(1)(iii), which stated that a covered entity that violated the satisfactory assurances it provided as a business associate would be in noncompliance with the Privacy Rule's business associate agreement provisions, as reflected by modified provision that directly restricts the uses and disclosures of protected health information by a business associate (including a covered entity acting as a business associate) to uses and disclosures allowed by the business associate agreement.[70] The Proposed Rule also sought to move the exceptions to a business associate to the definition itself.[71]

The Proposed Rule also eliminated the requirement that a covered entity report a material breach of the business associate's agreement to the Secretary, because under the Rule, a business associate may be held directly liable for certain violations of the business associate agreement, and both covered entities and business associates are required to report breaches of unsecured health information to the Secretary. Similarly, HHS proposed to require business associates aware of noncompliance by their business associate subcontractor to respond the same way that a covered entity must.[72]

The Proposed Rule also made changes to specific elements of the business associate agreement. According to the proposed rule, the business associate contract must require that:[73]

- Business associates comply with the Security Rule, regarding electronic protected health information;
- Business associates report breaches of unsecured protected health information to covered entities;
- Business associates ensure that subcontractors who receive or create protected health information be bound by the same restrictions and conditions that apply to business associates.

The Proposed Rule also provided that if a business associate was to carry out a covered entity's obligation, the business associate must comply with the Privacy Rule requirements that apply to covered entities. Furthermore, the proposed rule required business associates to enter into agreements with subcontractors that comply with the Privacy and Security Rules in the same way that covered entities are required to do with business associates.[74]

[69] 78 Fed. Reg. at 5599; 45 C.F.R. § 164.502(e).
[70] 78 Fed. Reg. at 5599; 45 C.F.R. § 164.502(e)(1)(iii).
[71] 78 Fed. Reg. at 5600; 45 C.F.R. § 160.103.
[72] 78 Fed. Reg. at 5600.
[73] 78 Fed. Reg. at 5600.
[74] 78 Fed. Reg. at 5600.

Key Provisions of the Final Rule

The Final Rule adopts the proposed modifications to the Privacy Rule.[75] While business associates are directly liable for impermissible uses or disclosures of protected health information, the Final Rule does not go so far as imposing all of the Privacy Rule's provisions on business associates.[76]

HHS notes that the business associate agreement is necessary to clarify the permissible uses and disclosures by the business associate as well as to ensure that the business associate is contractually required to perform certain activities for which direct liability does not attach. The agreement also clarifies the various obligations of the parties under HIPAA and notifies the business associate of its status under HIPAA so it is fully informed of its responsibilities and liabilities.[77]

The Final Rule adopts the Proposed Rule's language on documenting satisfactory assurances between covered entities and business associates as well as between business associates and subcontractors through a written contract or other agreement. The Final Rule also adopts the Proposed Rule's language requiring that any agreement between a business associate and a business associate subcontractor not allow the subcontractor to use or disclose protected health information that would not be permissible if done by the business associate.[78]

In the Final Rule, HHS adds language recognizing that a data use agreement may qualify as a business associate's satisfactory assurance that it will appropriately safeguard a covered entity's protected health information when the information is a limited data set.[79]

The Final Rule also retains language requiring business associates to comply with the applicable HIPAA rules for the covered entity when a business associate carries out a covered entity's obligations. The business associate agreement must specifically state that all obligations be carried out in compliance with the Privacy Rule. The Final Rule also applies the requirement that a business associate destroy all protected health information received from a covered entity to a subcontractor.[80]

Summary of Relevant Comments and HHS Response

Some comments suggested confusion over the need for business associate agreements, given the direct liability provision in the HITECH Act. HHS reaffirmed the need for business associate agreements, as it is required under HITECH.[81] There were also comments on what constituted satisfactory assurances.[82] HHS noted that the Privacy

[75] 78 Fed. Reg. at 5601; 45 C.F.R. §§ 164.502(e), 164.504(e).
[76] 78 Fed. Reg. at 5601.
[77] 78 Fed. Reg. at 5601.
[78] 78 Fed. Reg. at 5601.
[79] 78 Fed. Reg. at 5601-02; 45 C.F.R. § 165.504(e)(3)(iv).
[80] 78 Fed. Reg. at 5602; 45 C.F.R. § 164.504(e)(2)(ii)(H); §164.504(e)(2)-(4).
[81] 78 Fed. Reg. at 5600-01; HITECH Act § 13408.
[82] 78 Fed. Reg. at 5600.

Rule outlines the required provisions for the written agreement, and that specific elements are left up to the discretion of the covered entity and the business associate.[83] A few commenters also suggested that HHS provide a model business associate agreement.[84] HHS pointed out that it has published a sample business associate agreement on its website.[85]

In response to comments requesting guidance on whether a contract compliant with the Graham Leach Bliley Act (GLBA) and HIPAA rules could be used, HHS stated that one agreement may be used to satisfy the requirements of the HIPAA Rules and the GLBA.[86]

There were comments urging HHS to require business associates to disclose all subcontractors to a covered entity within 30 days and other comments advocating a certification process for HIPAA compliance for business associates and subcontractors. However, HHS declined to adopt these suggestions.[87]

Analysis

None.

45 C.F.R. § 164.532 -Transition Provisions

Relevant Statutory Provisions

HHS uses its regulatory authority to add a transition provision to establish the compliance date for modified standards.[88]

Key Provisions of the Proposed Rule

HHS proposed that covered entities and business associates be allowed to operate under their existing contracts for up to one year beyond the compliance date of the Final Rule, as long as the business associate and covered entity had an existing agreement with a business associate or subcontractor that complied with the prior provisions of the HIPAA Rules. For agreements between business associates and subcontractors, the Proposed Rule would grandfather the existing written agreements, which would be deemed to be in compliance with the Final Rule, until the covered entity or business associate modified the agreement following the compliance date of the Final Rule or for one year after the compliance date, whichever is sooner.[89]

[83] 78 Fed. Reg. at 5601; 45 C.F.R. § 164.504(e).
[84] 78 Fed. Reg. at 5600.
[85] 78 Fed. Reg. at 5601.
[86] 78 Fed. Reg. at 5601.
[87] 78 Fed. Reg. at 5602.
[88] 78 Fed. Reg. at 5602; 45 C.F.R. § 160.104(c).
[89] 78 Fed. Reg. at 5603.

Key Provisions of the Final Rule

Adopted as proposed. HHS declines to deem sufficient those contracts that were renegotiated to be in compliance with the HITECH that do not meet the revised terms of the Final Rule. Those agreements are subject to the one year transition period.[90]

Summary of Relevant Comments and HHS Response

Some commenters thought that the one year timeframe was not enough time for the transition. Other comments suggested that contracts that were renegotiated to be in compliance with the applicable provisions of the HITECH Act in February 2010 should be deemed to be in compliance as well. HHS decided that one year was sufficient, as this was the length of time given to entities to revise their agreements in 2002, which was successful.[91]

Analysis

None.

45 C.F.R. § 164.508: Uses and Disclosures for Which an Authorization is Required: Sale of Protected Information

Relevant Statutory Provisions

The HITECH Act adds another circumstance in which an individual's written authorization was needed - the sale of protected health information.[92] Specifically, HITECH prohibits a covered entity or business associate from receiving direct or indirect remuneration in exchange for the disclosure of protected health information unless the entity has received an individual's authorization to do so.[93] There are also exceptions to the authorization requirement when the purpose of the exchange is for:[94]

- Public health activities
- Research purposes
- Treatment
- Sale, transfer or consolidation of the covered entity for due diligence purposes
- Services rendered by a business associate pursuant to an agreement
- Providing an individual access to his or her protected health information
- Other purposes as deemed by the Secretary

Key Provisions of the Proposed Rule

[90] 78 Fed. Reg. at 5603; 45 C.F.R. § 164.532(d) and (e).
[91] 78 Fed. Reg. at 5603.
[92] 78 Fed. Reg. at 5603; HITECH Act § 13405(d).
[93] 78 Fed. Reg. at 5603; HITECH Act § 13405(d)(1).
[94] 78 Fed. Reg. at 5603-04; HITECH Act § 13405(d)(2).

The Proposed Rule added a provision to the Privacy Rule requiring a covered entity to obtain an authorization for any disclosure of protected health information in exchange for direct or indirect remuneration from or on behalf of the recipient of the information. The authorization would be required to state that the disclosure would lead to remuneration to the covered entity. The Proposed Rule also excluded some disclosures of protected health information for remuneration. The provisions would also apply to business associates.[95]

The Proposed Rule also requested comment on the redisclosure of protected health information obtained by a covered entity or business associate for remuneration if a valid authorization was obtained. The Proposed Rule also requested comment on the proposed exceptions noted above and whether other exceptions should be included. The exceptions for public health activities and research also included an additional provision to also except protected health information in limited data sets. For the exception relating to individual access to protected health information, HHS included in that exception, the provision of a reasonable, cost-based fee to gain access and expanded the exception to also apply to cost based-fees for additional requests for accounting of disclosures. Specifically, a covered entity may receive remuneration that reflects the cost to prepare and transmit the protected health information for permissible disclosures as long as the covered entity is not making a profit on the fee.[96]

Key Provisions of the Final Rule

In the Final Rule, HHS adopts the Proposed Rule's prohibition on the sale of protected health information, with some modifications[97] The Final Rule moves the prohibition on the sale of protected health information to Section 164.502(a)(5)(ii) and defines "sale of protected health information" as "a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information."[98] The Final Rule also clarifies that the definition of "sale" is not limited to instances where there is a transfer of ownership of the information, as HIPAA and the Privacy Rule apply without regard to ownership of data. However, sale of protected health information does not include instances where a covered entity receives a grant for things like research studies, even if the research results may contain disclosed protected health information. Similarly, the receipt of government funding to conduct a program is not considered a sale under the Rule, even if as part of the funding, the entity is required to report data, as is the case in the meaningful use program. The Final Rule concludes that the exchange of information through a health information exchange where a user fee is paid does not constitute a sale.[99]

[95] 78 Fed. Reg. at 5604.
[96] 78 Fed. Reg. at 5604-05.
[97] 78 Fed. Reg. at 5606.
[98] 78 Fed. Reg. at 5606; 45 C.F.R. §§ 164.502(a)(5)(ii), 164.502(a)(5)(ii)(B)(1).
[99] 78 Fed. Reg. at 5606.

The Final Rule also clarifies the scope of the term "remuneration." The Final Rule states that nonfinancial benefits are included in the prohibition of remuneration. The Final Rule also clarifies that the terms "direct" and "indirect" apply to how the remuneration is received, which is reflected in the definition. Therefore, a covered entity may not disclose protected health information for in kind benefits unless the disclosure falls within an exception.[100]

The Final Rule retains the broad exception for public health disclosures, but fails to limit the exception to disclosures where the covered entity only receives a cost based fee as remuneration to transmit the data. The Final Rule adopts the Proposed Rule's exception for research purposes in full, including the cost based fee limitation, as well as the Proposed Rule's exception for treatment and payment disclosures in full, the exception to the remuneration prohibition for transfer, merger or consolidation of a covered entity, the exception for disclosures otherwise allowed by law, and the exception for disclosure to provide individual access to his or her health information or an accounting of disclosures.[101]

The Final Rule clarifies that the permissible costs included as a reasonable cost-based fee for preparation and transmission of data include both direct and indirect costs, such as labor, materials, and supplies for copying and storing, labor and materials to ensure information is disclosed in a permissible manner, and related capital and overhead costs. The Final Rule makes clear that fees that would allow an entity to incur a profit are not permissible.[102] The Final Rule permits the same types of costs that are allowed under the research exception as permissible reasonable cost-based fees, as well as costs that are in compliance with state-based fee schedules, including direct or indirect costs, such as labor and supplies to prepare and transmit the data.[103] The Final Rule also adopts the exceptions for remuneration paid by a covered entity to a business associate for activities performed on behalf of the covered entity or remuneration as a cost based fee to cover the cost to prepare and transmit protected health information for a permitted disclosure. The Final Rule adds business associates as also being allowed to receive remuneration as a cost- based fee to prepare or transmit protected health information, and allows business associates to recoup fees from third party record requestors to cover the cost to prepare and transmit the information. The Final Rule clarifies that pursuant to the business associate exception, a business associate could provide remuneration to a subcontractor for activities performed on behalf of the business associate. Finally, the Final Rule includes business associates in the general prohibition against the sale of protected health information for consistency.[104]

The Final Rule also clarifies that redisclosure of protected health information for remuneration by a covered entity or business associate requires an additional

[100] 78 Fed. Reg. at 5607.
[101] 78 Fed. Reg. at 5607.
[102] 78 Fed. Reg. at 5607.
[103] 78 Fed. Reg. at 5607-08.
[104] 78 Fed. Reg. at 5607.

authorization unless the original authorization is clear that the covered entity or business associate will further disclose the information.[105]

Summary of Relevant Comments and HHS Response

Many commenters asked for clarification as to the scope of what constitutes "the sale of protected health information." Some comments reflected the need for HHS to include a definition of "sale of protected health information," which HHS did in the Final Rule.[106] Commenters also expressed concern that fees paid for services that involve the disclosure of protected health information but do not include the purchase of data, would nevertheless be considered a sale of protected health information. HHS addressed this concern in the Final Rule as well.[107] Other comments reflected the concern over authorization requirements for sale of protected health information while applying for funding that would require the reporting of data, such as the Medicare and Medicaid meaningful use program, which HHS stated is not considered a sale.[108] There was also concern over the meaning on "indirect remuneration," including whether it meant nonfinancial benefits provided in exchange for protected health information would turn a disclosure into a sale. Commenters suggested that the authorization requirement for indirect remuneration would discourage covered entities from participating in collaborative research or quality activities where they may receive indirect remuneration for contributing data to a central database. Nevertheless, HHS clarified in the Final Rule that indirect remuneration applies to how it is received, and not the type of remuneration, as nonfinancial benefits are included in the prohibition.[109]

There was significant support for the broad public health exception to the remuneration prohibition and the limited data set provision, which HHS retained.[110] In general, commenters were opposed to the restriction on the remuneration being limited to the cost of preparing and transmitting the protected health information because it would discourage covered entities from making public health related disclosures. The comments reflected the same ideas for the research exception.[111] However, the Final Rule clarified that reasonable cost-based fees may include direct or indirect costs.[112] There were a number of comments on the proposed exception allowing business associates to receive payments of costs from third parties for providing services processing requests for medical record copies on behalf of covered entities, which the Final Rule clarified.[113] Similarly, commenters supported the exception to the remuneration prohibition for treatment and payment purposes, the exception for sale,

[105] 78 Fed. Reg. at 5608.
[106] 78 Fed. Reg. at 5605; 45 C.F.R. § 164.502(a)(5)(ii)(B)(1).
[107] 78 Fed. Reg. at 5605-06.
[108] 78 Fed. Reg. at 5605-06.
[109] 78 Fed. Reg. at 5605, 5607.
[110] 78 Fed. Reg. at 5605-07.
[111] 78 Fed. Reg. at 5606.
[112] 78 Fed. Reg. at 5607-08.
[113] 78 Fed. Reg. at 5606, 5607.

transfer or merger of a covered entity, and the exception for a legal obligation to disclose protected health information.[114]

As requested in the comments, the Final Rule will grandfather in prior authorizations for research use or disclosure so that the studies are not interrupted.[115] The Final Rule added a provision that allows a covered entity to rely on an authorization given prior to the compliance date of the final rule even if remuneration is involved, but the remuneration is not included in the disclosure.[116] The Final Rule also added a provision that allows a covered entity to use or disclose a limited data set based on its existing data use agreement, including for research purposes, until it is renewed, modified or one year from the compliance date of the rule, whichever is earlier.[117]

In response to comments that the prohibition on the sale of protected health information would prevent a covered entity from disclosing information to a collection agency without authorization, the Final Rule clarified that such a disclosure is permissible under the payment exception to the rule. In response to comments concerning the implication of the authorization requirement when a covered entity is going through a reorganization or transfers of values among entities under common control, the Final Rule clarified that the authorization requirement applies to disclosures outside of a covered entity, and that covered entities organized as "affiliated covered entities," are not impacted by the authorization provisions.[118]

The Final Rule responded to concerns over an IRB's role in determining the reasonableness of the cost based fee by stating that the covered entity and/or the business associate is responsible for making this determination.[119]

To clarify the different obligations to provide access to protected health information versus statistical data, the Final Rule stated that a disclosure of de-identified information is not subject to the remuneration prohibition. Some commenters felt that limited data sets should likewise be exempted from remuneration prohibition because they are not fully identifiable, but HHS disagreed, stating that limited data sets are still protected health information.[120]

Analysis

None.

45 C.F.R. § 164.508(b)(3) – Compound authorizations

[114] 78 Fed. Reg. at 5605-06.
[115] 78 Fed. Reg. at 5608.
[116] 78 Fed. Reg. at 5608; 45 C.F.R. § 164.502(a)(4).
[117] 78 Fed. Reg. at 5608; 45 C.F.R. § 164.532(f).
[118] 78 Fed. Reg. at 5608.
[119] 78 Fed. Reg. at 5608-09.
[120] 78 Fed. Reg. at 5609.

Relevant Statutory Provisions

HHS using its regulatory authority.

Key Provisions of the Proposed Rule

Section 164.508(b)(3) generally prohibits the use of "compound authorizations" (i.e., an authorization of the use and disclosure of protected health information that is combined with any other legal permission). However, Section 164.508(b)(3)(i) carves out an exception by permitting the combining of an authorization for use and disclosure of protected health information in a research study with any other permission for the same study, including participation in the study.[121]

Section 164.508(b)(4) generally prohibits covered entities from conditioning treatment, payment, enrollment in a health plan, or eligibility of benefits on the provision of an authorization (a conditioned authorization) with certain exceptions, including the research context. An example is when the provision of research-related treatment is conditioned on obtaining an individual's authorization. Section 164.508(b)(3)(iii) limited the use of compound authorizations by prohibiting the combining of a conditioned authorization with an unconditioned authorization (i.e., an authorization for another purpose for which treatment, payment, enrollment, or eligibility may not be conditioned). This was intended so that individuals understand that they may decline the activity described in the unconditioned authorization while still receiving treatment or other services or benefits by agreeing to the conditioned authorization.[122]

Various groups, including researchers and professional organizations, had previously expressed concern that the approach of the prior rule lacked integration and created unnecessary documentation burdens. An example of the effect of these limitations could be seen during research trials that are associated with a corollary research activity, such as when protected health information is used or disclosed to create or contribute to a central research database or repository. For example, a clinical trial which includes both the provision of treatment and tissue banking of collected specimens (and its associated protected health information) would require separate authorizations. Members of the research community have stated that multiple authorizations could potentially confuse research subjects and/or dissuade them altogether from participating in a clinical trial. They have also noted that requiring separate forms for such corollary research activities is inconsistent with current practice for obtaining informed consent under the Common Rule.[123, 124]

[121] 78 Fed. Reg. at 5609.
[122] 78 Fed. Reg. at 5609.
[123] See 45 C.F.R. pt. 46 for the Common Rule.
[124] 78 Fed. Reg. at 5609-10.

In light of these concerns, the Secretary's Advisory Committee on Human Research Protections in 2004[125] and the Institute of Medicine in its 2009 Report[126] made specific recommendations to allow combined authorizations in one form for clinical trials and related biospecimen storage. The Proposed Rule sought to address these concerns by amending Sections 164.508(b)(3)(i) and (iii) to allow a covered entity to combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities. The Proposed Rule also aimed to streamline the process for obtaining an individual's authorization for research and to allow covered entities to have some flexibility with respect to how they meet the authorization requirements.[127]

Key Provisions of the Final Rule

The Final Rule is adopted as proposed. The Final Rule allows for the use of compound authorizations for any type of research activities, not just clinical trials or biospecimen banking, as well as permits future secondary use of protected health information (to the extent the future use authorization is in compliance with Section 164.508(c) and the modified interpretation of HHS under the Final Rule). However, the limitations on an authorization for a use or disclosure of psychotherapy notes pursuant to Section 164.508(b)(3)(ii) remains unchanged. In addition, HHS declines to permit a combined authorization that only allows the individual the option to opt out of the unconditioned research activities (e.g., "check here if you do NOT want your data provided to the biospecimen bank") because an opt out option would not provide individuals with clear enough ability to authorize the optional research activity, as well as potentially being viewed as coercive by individuals.[128]

The Final Rule does not remove or reduce the required elements of an authorization, but is intended to reduce potential confusion among research subjects caused by the use of multiple authorization forms and to help covered entities, institutions, and institutional review boards with flexibility, avoidance of redundant language, and to align the authorization requirements under the Privacy Rule with what has been common and ongoing practice with respect to informed consent forms under the Common Rule. Covered entities are permitted but not required by these modifications to use compound authorizations for conditional and unconditional research activities.[129]

Summary of Relevant Comments and HHS Response

[125] See Letter dated September 27, 2004 to the Secretary of HHS (Recommendation V), available at http://www.hhs.gov/ohrp/sachrp/hipaalettertosecy090104.html.
[126] See Institute of Medicine, "Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research" (Recommendation II.B.2), released January 27, 2009, available at http://www.iom.edu/Reports/2009/Beyond-the-HIPAA-Privacy-Rule-Enhancing-Privacy-Improving-Health-Through-Research.aspx.
[127] 78 Fed. Reg. at 5609-10.
[128] 78 Fed. Reg. at 5610.
[129] 78 Fed. Reg. at 5610-11.

Among commenters, almost all strongly supported the proposal to allow combined authorizations for conditioned and unconditioned research activities. Many also supported allowing flexibility to covered entities and institutions to determine how best to present the authorizations and differentiate conditioned versus unconditioned activities. Support in these respects came from the Secretary's Advisory Committee on Human Research Protections, expressing particular appreciation for the goal of harmonization with the Common Rule.[130]

Several commenters suggested that an opt-out method should be allowed as an alternative to an opt-in method. For the reasons described above, HHS declines to permit use of an opt-out method. A few commenters opposed altogether the proposal to allow combined authorizations for conditioned and unconditioned research activities, generally feeling that separate authorizations were appropriate and that there was insufficient evidence to suggest that combining forms would be beneficial to individuals. However, the majority of commenters supported the Proposed Rule.[131]

HHS clarified in its response to comments that the modified compound authorization provision does not affect the waiver of authorization provisions in the Privacy Rule if the requirements of Section 164.512(i) have been met, indicating that an institutional review board has waived the obtaining of individual authorization for such purposes. HHS also clarified that a clear revocation by an individual of only one part of a compound authorization does not equate to a revocation of the entire authorization. However, if it is not clear exactly which part of the research activities the individual's revocation applies to, then written clarification must be obtained from such individual. Otherwise, the entire authorization must be treated as revoked.[132]

Analysis

The modified compound authorization provisions of the Final Rule should allow covered entities, institutions, and institutional review boards to streamline the authorization process by allowing flexibility in designing an authorization that is better tailored to the research study at hand, including any corollary research activities such as biospecimen use and storage. These provisions under the Privacy Rule are now better aligned with the informed consent form requirements under the Common Rule. Overall, reducing administrative burdens should enhance the clinical research efforts of both researchers and individuals who are interested in participating in research while still balancing the protection of health information.

45 C.F.R. § 164.508(c)(1)(i) [HHS interpretation as it Relates to Authorizing Future Research Use or Disclosure]

Relevant Statutory Provisions

[130] 78 Fed. Reg. at 5610.
[131] 78 Fed. Reg. at 5610.
[132] 78 Fed. Reg. at 5611.

HHS using its regulatory authority.

Key Provisions of the Prior Interpretation

In the context of obtaining health information for purposes of future research, HHS previously interpreted Section 164.508(c)(1)(i) of the Privacy Rule to require authorizations for research to be study specific and include a description of each purpose of the requested use and disclosure. There was concern that patients would lack necessary information in the authorization to make an informed decision about the future research. However, HHS heard many concerns from covered entities and researchers that this interpretation encumbered secondary research and limits an individual's ability to authorize the use or disclosure of protected health information for future research. Commenters also noted that this interpretation diverged from current practice under the Common Rule, which allows a researcher to seek from a research subject informed consent to future research so long as the uses in future research are described in sufficient detail to allow for an informed consent.[133]

In the Proposed Rule, HHS solicited comments on options regarding authorizations for future research, including whether the Privacy Rule should: (i) permit an authorization for future research purposes to the extent such purposes are adequately described in the authorization and that an individual could reasonably expect to have his or her protected health information used or disclosed for such future research, or (ii) permit an authorization for future research purposes but require certain specific elements or statements to be made to individuals, particularly regarding any sensitive research activities, such as genetic analyses or mental health research, that may affect their willingness to participate in the research.[134]

Key Provisions of the Modified Interpretation

HHS is modifying its interpretation of the "purpose" provision at Section 164.508(c)(1)(i) such that an authorization for the use or disclosure of protected health information for research purposes need no longer be study specific. This modified interpretation does not change the authorization requirements of Section 164.508, which includes requiring a description of each purpose of the requested use or disclosure. However, under this modified interpretation, an authorization requested for future research purposes can be made by including adequate description of such purposes so that it would be reasonable for an individual to expect that his or her protected health information could be used or disclosed for future research. Such a description could include specific statements about sensitive research activities to the extent such research is contemplated.[135]

By not requiring any specific statements to comply with Section 164.508(c)(1)(i) with regard to authorizations for future research, HHS agreed with commenters who stated that it is difficult to define what is sensitive and the concept changes over time. HHS also

[133] 78 Fed. Reg. at 5611-12.
[134] 78 Fed. Reg. at 5612.
[135] 78 Fed. Reg. at 5612.

intended for this approach to harmonize with practice under the Common Rule regarding informed consent for future research.[136]

HHS had also solicited comments on how a revocation would operate with respect to future research. Several commenters suggested that revocation of authorizations should continue to be permitted in the same manner that is currently allowed under the Privacy Rule. HHS agreed with this approach and covered entities may continue to rely on existing guidance regarding the operation of revocations in the research context.[137]

Summary of Relevant Comments and HHS Response

Almost all commenters supported the proposal to allow authorizations for future research. Many commenters indicated the importance of flexibility, including about half who wanted maximum flexibility for covered entities, institutions, and institutional review boards to determine the appropriateness and adequacy of descriptions of future research. These commenters supported the first proposed option described above but not the second, requiring specific statements. The Secretary's Advisory Committee on Human Research Protections also agreed with the need for flexibility and to harmonize the Privacy Rule requirements with practice under the Common Rule.[138]

Several commenters specifically opposed requiring specific statements about sensitive research in authorizations, expressing concerns about variability in what may constitute sensitive information or sensitive research activities and practicality challenges. A few commenters opposed the proposal to allow authorizations for future research altogether. Some of these commenters felt very strongly, in the interest of protecting patients, that it would be impossible for any individual to be truly informed about future research.[139]

Analysis

This modified interpretation, which allows the authorization of use or disclosure of protected health information for future research purposes if the delineated requirements are met, will allow additional flexibility for covered entities, institutions, and institutional review boards. This approach will also harmonize the Privacy Rule with practice under the Common Rule regarding informed consent for future research. These changes enhance research efforts for both researchers and individuals who are interested in participating in research, including future research, while still balancing the protection of health information.

45 C.F.R. § 164.502(f) – Standard: Deceased Individuals; 45 C.F.R. § 160.103 – Definition of "Protected Health Information"

Relevant Statutory Provisions

[136] 78 Fed. Reg. at 5612.
[137] 78 Fed. Reg. at 5613.
[138] 78 Fed. Reg. at 5612.
[139] 78 Fed. Reg. at 5612.

HHS using its regulatory authority.

Key Provisions of the Proposed Rule

Previously, Section 164.502(f) required covered entities to protect a decedent's protected health information generally in the same manner and to the same extent as the protected health information of living individuals. In order to use or disclose a decedent's protected health information for a particular purpose, a covered entity would have to obtain authorization from the decedent's personal representative (the executor, administrator, or other person who is legally authorized to act on behalf of the decedent or the decedent's estate). The Proposed Rule sought to amend Section 164.502(f) such that the protection of a decedent's protected health information under the Privacy Rule would only be extended for a period of 50 years following the date of death. For consistency, the Proposed Rule also sought to amend the definition of "protected health information" under Section 160.103 to exclude individually identifiable health information regarding a person who has been deceased for more than 50 years.[140]

HHS has received a number of concerns since the publication of the Privacy Rule about the difficulties of locating personal representatives to obtain authorization for the use or disclosure of a decedent's protected health information, especially after closure of the decedent's estate. Historical researchers such as archivists, biographers, and historians had also expressed frustration regarding the lack of access to old or ancient records of historical value in the possession of covered entities subject to the Privacy Rule.[141]

Key Provisions of the Final Rule

The Final Rule is adopted as proposed. HHS believes that the 50 year time period is an appropriate period of protection for decedent health information that balances the remaining privacy interests of living relatives or other affected individuals with a relationship to the decedent with the difficulty of obtaining authorization from the personal representative of a decedent as time passes.[142]

Summary of Relevant Comments and HHS Response

The majority of comments were in favor of the Proposed Rule. Some of these commenters even stated that the 50 year time period was too long and should be shortened to, for example, 25 years. However, HHS believed that a 50 year time period (spanning approximately two generations) represents the appropriate balance with 25 years being too short of a time period and 75 or 100 years being too long.[143]

[140] 78 Fed. Reg. at 5613-14.
[141] 78 Fed. Reg. at 5613-14.
[142] 78 Fed. Reg. at 5614.
[143] 78 Fed. Reg. at 5614.

Some commenters were opposed to the Proposed Rule, stating that living relatives, as well as the decedents, had a continuing privacy interest in the decedent's health information, especially if it involves highly sensitive information, such as HIV/AIDS, substance abuse, or mental health information or psychotherapy notes. However, HHS believed that state or other laws may require greater privacy protections than under HIPAA. A few commenters were concerned that the 50 year period of protection could be interpreted as a proposed record retention requirement. This concern was rejected by HHS.[144]

Analysis

The prior rule that a decedent's protected health information had to be protected in the same manner and to the same extent as the protected health information of a living individual was too restrictive and did not take into consideration the potential for historic or academic interest in a decedent's health information. Limiting the requirement for a covered entity to protect a decedent's protected health information to a period of 50 years following the date of death strikes some balance between the remaining privacy interests of living individuals and any historic value or interest in the decedent's protected health information. However, whether a 50 year time period versus a longer or shorter time period strikes the optimal balance is yet to be tested. Overall, this amendment may not affect a large number of covered entities or individuals.

45 C.F.R. § 164.510(b) – Standard: Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes; 45 C.F.R. § 160.103 – Definition of "Family Member"

Relevant Statutory Provisions

HHS using its regulatory authority.

Key Provisions of the Proposed Rule

Section 164.510(b) describes how a covered entity may use or disclose protected health information to family members or others who are involved in an individual's health care or payment related to such care. The Proposed Rule sought to add a new paragraph to Section 164.510(b) that would permit a covered entity to use or disclose a decedent's health information to family members or others who were involved in the decedent's health care or payment for care prior to death, unless doing so would be inconsistent with any prior expressed preference of the individual that is known to the covered entity. The Proposed Rule was intended to address questions and concerns heard from family members, relatives, and others, many of whom had access to an individual's health information during his or her care, but then had difficulty obtaining information after the death of the individual because they did not qualify as a "personal representative" under Section 164.502(g)(4).[145]

[144] 78 Fed. Reg. at 5614.
[145] 78 Fed. Reg. at 5614-15.

Key Provisions of the Final Rule

The Final Rule is adopted as proposed, including the addition of the definition of "family member" at Section 160.103. HHS believes that the Final Rule strikes an appropriate balance in allowing covered entities to communicate with family members and others who were involved in the health care or payment for care of an individual prior to his or her death following that person's death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.[146]

The Final Rule will allow family members and others to learn about the circumstances surrounding the death of a loved one, unless that person had objected to the covered entity making such communications prior to his or her death. Examples may include a covered health provider describing to a decedent's sister the circumstances of her sibling's death or disclosing billing information so she may help wrap up her sibling's estate. HHS states that in both of these types of cases, the provider generally should not share information about the decedent's past, unrelated medical problems. It also clarifies that these are permitted, but not required, disclosures. If a covered entity believes that, based on the circumstances, a disclosure of a decedent's protected health information would be inappropriate, it is not required to make the disclosure.[147]

Summary of Relevant Comments and HHS Response

Most commenters supported the Proposed Rule, feeling that permitting such disclosures would help facilitate important and appropriate communications between providers and family members and others who had been involved in the care or payment for care of a loved one prior to that individual's death but whose status may not rise to the level of a "personal representative" under the Privacy Rule. A few commenters opposed the amendment.[148]

Two commenters believed that covered entities would have too large of a burden to determine the legitimacy of a requestor as a family member or other person involved in the decedent's care or payment for care. One commenter even suggested including language in the Final Rule that would put the burden of proof to show "involvement in the individual's care" on the requestor. HHS declined to include such language because it believed that existing guidance on similar disclosures by providers to family members and others who are involved in the health care or payment for care of a living individual as permitted under Section 164.510(b) is sufficient. The covered entity need only have "reasonable assurance" that the family member or other individual was involved in the decedent's care or payment for care prior to death, which in some cases will be readily apparent. Depending on the circumstances, disclosure might be made to spouses, parents, children, domestic partners, other relatives, or friends of the decedent.[149]

[146] 78 Fed. Reg. at 5615.
[147] 78 Fed. Reg. at 5615.
[148] 78 Fed. Reg. at 5615.
[149] 78 Fed. Reg. at 5615-16.

Analysis

The Final Rule will provide greater flexibility to covered entities to communicate important information to family members and others of a decedent who were involved in the care or payment for care of their loved one. It should also ease frustration for many family members and others who might otherwise face resistance from a covered entity or health care provider to disclose a decedent's information because they are concerned with maintaining compliance with the Privacy Rule. The Final Rule recognizes the continuing privacy interest in a decedent's protected health information. However, it also recognizes that there is a lesser privacy interest in a decedent's protected health information compared to a living individual's protected health information and that there are certain circumstances when the interests of living individuals in a decedent's protected health information should trump. In this sense, the Final Rule is also consistent with the change to Section 164.502(f) discussed above regarding the limited period of protection for a decedent's protected health information.

45 C.F.R. § 164.512(b) – Standard: Uses and Disclosures for Public Health Activities

Relevant Statutory Provisions

HHS using its regulatory authority.

Key Provisions of the Proposed Rule

Section 164.512(b) permits covered entities to disclose the minimum necessary protected health information of individuals to public health authorities or other designated persons or entities without an authorization for public health purposes by recognizing the need to balance the privacy interests in the health information of individuals with the sharing of health information between covered entities and those responsible for ensuring public health and safety. The Proposed Rule sought to add an additional permitted use under Section 164.512(b)(1) for covered entities to disclose proof of immunization to schools where state or other law requires the school to have such information prior to admitting the student. Covered entities would be required to obtain agreement from a parent, guardian, or other person acting *in loco parentis*, however, the agreement could be oral and need not be a written authorization. The Proposed Rule was intended to ease the burden on schools, covered entities, and parents to get school-aged children immunized and proof of their immunization to the schools, which play an important public health role in preventing the spread of communicable diseases.[150]

HHS requested comment on whether an oral agreement should still be documented by the covered entity. It also requested comment on whether "school" should be defined and whether the rules should mandate that immunization disclosures go to a particular school official.[151]

[150] 78 Fed. Reg. at 5616.
[151] 78 Fed. Reg. at 5616.

Key Provisions of the Final Rule

The Final Rule is adopted as proposed with the addition that a covered entity will need to obtain and document agreement from a parent, guardian, or other person acting *in loco parentis* for the student, or the student him- or herself if an adult or emancipated minor. However, the agreement need not be a written authorization. HHS believes that the option for parents to provide, and for covered entities to accept, oral agreements will relieve the burden on all parties concerned. For example, a parent or guardian could simply make a phone call or send an email to their provider requesting that their child's immunization records be disclosed to the child's school. This agreement would be considered effective until revoked.[152]

Summary of Relevant Comments and HHS Response

Most commenters generally favored the Proposed Rule with the intent to ease the burden of covered entities and parents, guardians, or other persons acting *in loco parentis* to disclose proof of immunization to schools. However, commenters were divided on whether written documentation of agreement should be required or not. Comments were also divided on whether an agreement was needed at all. Some commenters thought that requiring any agreement would be unnecessary, confusing, and burdensome. Some commenters suggested that disclosure of immunization records should be considered an exempt public health disclosure.[153]

Commenters who were in favor of using oral agreements were divided on whether written documentation of the oral agreement should be required. Some felt that requiring written documentation of an oral agreement would be as burdensome as requiring written agreement or written authorization. HHS ultimately agreed with those commenters who believed that agreement from a parent or guardian was still necessary but that permitting oral agreement would reduce the burden. It also agreed with those commenters who believed that documentation by covered entities of an oral agreement would not be as burdensome as requiring a written agreement. For example, the covered entity could make a notation in the child's medical chart or save a copy of the email request from a parent. As some commenters pointed out, covered entities are already incentivized to document oral agreements for their own liability purposes.[154]

The Final Rule does not include a definition of "school." HHS agreed with commenters who believed that the term "school" should remain undefined in the Privacy Rule due to the variation across states in the types of schools that are subject to entry laws. Most commenters also felt that if the term "school" was to be defined, that it should be defined broadly in order to best support public health efforts. In addition, the Final Rule does not define "school official" nor does it otherwise mandate who would be an appropriate person at the school to receive immunization disclosures from covered entities. The

[152] 78 Fed. Reg. at 5617.
[153] 78 Fed. Reg. at 5616-17.
[154] 78 Fed. Reg. at 5617.

majority of commenters requested that a designated recipient of student immunization records be left undefined to allow schools flexibility to identify the appropriate person(s). One commenter requested designation of the school nurse. However, not all schools have a school nurse or one who is available full-time.[155]

Several commenters raised concerns about the dynamic between the Privacy Rule and state laws requiring immunization disclosures. HHS clarified that the Privacy Rule does not prohibit state law mandated disclosures of immunization information, nor does it require authorization for such disclosures. With respect to state immunization registries, it clarifies that disclosures of protected health information to such registries are also permitted by the Privacy Rule as a disclosure for public health purposes and does not require authorization.[156]

Analysis

The Final Rule will reduce the burden on schools, covered entities, and parents, guardians, or other persons acting *in loco parentis* to get school children immunized and proof of immunization to the schools. Covered entities will have flexibility in how they document oral agreements and schools will have flexibility in whom they designate to receive and collect immunization disclosures. In addition to helping schools fulfill one of their public health functions, the Final Rule may also help prevent children from missing days in school or otherwise suffering delays in attending school due to delays in getting their immunization information from covered entities to the schools. Furthermore, HHS has attempted to avoid confusing or conflicting requirements in the Privacy Rule as they may relate to state laws that require immunization disclosures.

45 C.F.R. § 164.514(f) – Fundraising Communications; 45 C.F.R. § 164.520(b)(1)(iii)(A) – Separate Statements for Certain Uses or Disclosures

Relevant Statutory Provisions

HITECH Act Section 13406(b) requires that a covered entity provide the recipient of a fundraising communication with a clear and conspicuous opportunity to opt out of receiving any further fundraising communications. In addition, if an individual does opt out, the choice must be treated as a revocation of authorization under Section 164.508 of the Privacy Rule.[157]

Key Provisions of the Proposed Rule

Generally, Section 164.514(f)(1) of the Privacy Rule permits a covered entity to use, or to disclose to a business associate or an institutionally related foundation, certain types of protected health information about an individual for the covered entity's fundraising from that individual without the individual's authorization. The Privacy Rule also requires a

[155] 78 Fed. Reg. at 5618.
[156] 78 Fed. Reg. at 5618.
[157] 78 Fed. Reg. at 5618-19.

covered entity that plans to use or disclose such protected health information for fundraising to inform individuals in its notice of privacy practices that it may contact them to raise funds for the covered entity. The prior rule also required that a covered entity must only make "reasonable efforts" to ensure that individuals who opted out of receiving fundraising communications would not be sent future communications.[158]

The Proposed Rule introduced several changes to the fundraising requirements under the Privacy Rule in order to implement HITECH Act Section 13406(b), including the following:

- Strengthened the opt out option by requiring that covered entities provide, with each fundraising communication sent to an individual under these provisions, a "clear and conspicuous" opportunity for the individual to elect not to receive further fundraising communications;
- The method for an individual to opt out may not cause the individual to incur undue burden or more than nominal cost;
- Covered entities may not condition treatment or payment on an individual's choice whether to receive fundraising communications;
- Covered entities may not send fundraising communications to an individual who has opted out (the "reasonable efforts" language was removed); and
- The fundraising statement required under the provisions for notice of privacy practices must not only notify individuals that they may be contacted about fundraising, but that they also have a right to opt out of receiving such fundraising communications.[159]

The Proposed Rule also requested public comment on several aspects regarding application and workability of the fundraising requirements under the Privacy Rule, including the following:

- What fundraising communications the opt out should apply to, whether all future communications or could the opt out be structured in a way as to only apply to particular fundraising campaigns that have been described;
- Whether the Privacy Rule should allow a similar method, less burdensome than written authorization, so that individuals could opt back in to receive a covered entity's fundraising communications after having previously opted out;
- What other limited types of protected health information, if any, should be added to the list under Section 164.514(f)(1) beyond demographic information and dates of health care service that a covered entity may use or disclose to more effectively target fundraising without an authorization; and
- Whether it would be workable to require covered entities to provide individuals an opportunity to opt out of receiving fundraising communications before making the first fundraising communication (a "pre-solicitation opt out").[160]

[158] 78 Fed. Reg. at 5618-19.
[159] 78 Fed. Reg. at 5618-19.
[160] 78 Fed. Reg. at 5618-19.

HHS also considered the recommendations of the National Committee on Vital and Health Statistics summarized in a letter to the Secretary of HHS dated September 2, 2004,[161] which included (i) allowing covered entities to use or disclose information related to an individual's department of service (broad designations, such as surgery or oncology) for fundraising activities, and (ii) including language in the notice of privacy practices to inform patients that their department of service information may be used in fundraising and that they would have an opportunity to opt out of the use or disclose of such information.[162]

Key Provisions of the Final Rule

The Final Rule is adopted as proposed. In addition, HHS amends Section 164.514(f)(1) to allow certain additional categories of protected health information to be used or disclosed for fundraising purposes without an authorization. Besides demographic information and dates of health care service, which were already allowed under the prior rules, information as to department of service, treating physician, outcome information, and health insurance may now be used or disclosed for fundraising. This addresses the categories cited by most commenters as necessary to target fundraising communications to appropriate individuals. Demographic information relating to an individual has also been clarified to include name, address, contact information, age, gender, and date of birth.[163]

New Section 164.514(f)(2)(v) allows a covered entity to provide individuals who have previously opted out of receiving fundraising communications a method to opt back in. The Final Rule gives covered entities the flexibility and discretion to determine what type of method to employ, which need not be a signed authorization.[164]

Summary of Relevant Comments and HHS Response

Commenters were generally supportive of the Proposed Rule, however, many requested that covered entities be given flexibility to implement the requirements and determine which methods would work best given their own circumstances. The vast majority of commenters supported allowing the use or disclosure of greater categories of protected health information for fundraising purposes, stating that it would allow covered entities to streamline their fundraising efforts and to better target individuals by sending them communications that would be more meaningful to their experiences. It would also help eliminate the concern of sending a communication to an individual or family member who suffered a negative outcome such as, for example, death or disability.[165]

With regard to the provision prohibiting covered entities from conditioning treatment or payment on an individual's choice whether to receive fundraising communications, most

[161] See letter at http://www.ncvhs.hhs.gov/040902lt1.htm.
[162] 78 Fed. Reg. at 5619.
[163] 78 Fed. Reg. at 5620-22.
[164] 78 Fed. Reg. at 5620-22.
[165] 78 Fed. Reg. at 5619-20.

commenters generally supported this modification. However, most commenters opposed the provision prohibiting covered entities from sending future fundraising communications to those individuals who had opted out as being too strict and very difficult for covered entities to ensure 100% accuracy. The majority of these commenters preferred to retain the original "reasonable efforts" standard.[166] In the Final Rule, HHS retains the language of the Proposed Rule and eliminates the "reasonable efforts" language, which it considers more protective of individuals' rights and consistent with the requirements of the HITECH Act. The expectation is that covered entities will use the same level of care and handling in the use or disclosure of protected health information in fundraising as is necessary in all other health care operations.[167]

With regard to the requirement that the method for an individual to opt out of receiving fundraising communications should not cause the individual to "incur an undue burden or more than nominal cost," HHS generally agreed with those commenters who stated that covered entities should be given flexibility to determine what type of method to use. Multiple methods or a single method can be used. Methods that should be considered include toll-free phone numbers, an email address, prepaid, pre-printed postcards, or similar approaches that are simple, quick, and inexpensive for individuals wishing to opt out. However, requiring individuals to write and send a letter to the covered entity in order to opt out will be considered an undue burden by HHS. Covered entities are also encouraged to consider the size of their population, geographic distribution, and any other factors that may help determine the most appropriate and least burdensome opt out method.[168]

With regard to the scope of the opt out, covered entities have been given flexibility and discretion to determine whether an opt out by an individual will apply to all future communications or only to specific fundraising campaigns (if the covered entity has the ability to track campaign-specific opt outs). Commenters were split on this particular issue. Covered entities may also provide individuals with the choice of opting out of all future or just campaign-specific communications. However, HHS declined to require pre-solicitation opt outs because of the additional cost and burden to covered entities. It also believes that the modified language in the notice of privacy practices will sufficiently inform individuals that they may be contacted for fundraising purposes and that they will have an opportunity to opt out.[169]

A few commenters preferred the adoption of an opt in process rather than an opt out process for individuals to consent to and receive fundraising communications. However, HHS declined to require an opt in process, noting that the HITECH Act did not replace the opt out process with an opt in process.[170] In addition, all commenters were opposed to requiring covered entities to provide a pre-solicitation opt out to individuals.[171]

[166] 78 Fed. Reg. at 5620.
[167] 78 Fed. Reg. at 5621.
[168] 78 Fed. Reg. at 5620-21.
[169] 78 Fed. Reg. at 5620-22.
[170] 78 Fed. Reg. at 5622.
[171] 78 Fed. Reg. at 5620.

Analysis

While strengthening the privacy rights of individuals who choose to opt out of receiving fundraising communications, the Final Rule affords to covered entities a large amount of flexibility and discretion to determine the best methods to employ in order to meet their obligations under Section 164.514(f) of the Privacy Rule. The Final Rule attempts to balance the interests of individuals and covered entities in the fundraising context, while keeping within the letter and spirit of Section 13406(b) of the HITECH Act.

45 C.F.R. § 164.520 – Notice of Privacy Practices for Protected Health Information.

Relevant Statutory Provisions

Notice of the rule regarding breach notification of unsecured protected health information under Section 13402 of the HITECH Act (the "***Breach Notification Rule***")[172]

Key Provisions of the Proposed Rule

Section 164.520 of the Privacy Rule requires most covered entities to provide individuals with a notice of the privacy practices (NPP) that the covered entity must follow.[173] The NPP must describe the uses and disclosures of protected health information that a covered entity is permitted to make, its legal duties and privacy practices with respect to such information, and the individual's rights regarding his or her own protected health information. The Proposed Rule introduced several material modifications to the required content of NPPs, including the following:

- Require that the NPP describe the uses and disclosures of protected health information that require an authorization under Section 164.508(a)(2) through (a)(4) (i.e., include a statement that most uses and disclosures of psychotherapy notes and of protected health information for marketing purposes and the sale of protected health information require an authorization), and provide that other uses and disclosures not described in the NPP will be made only with the individual's authorization;[174]
- Require covered health care providers to notify individuals in the NPP of the provider's intent to send treatment communications to individuals where the provider receives financial remuneration[175] in exchange for making such communications (i.e., "subsidized treatment communications") and to inform individuals that they can opt out of receiving such communications;[176]
- Require covered entities that intend to send fundraising communications to individuals to notify individuals in the NPP of this intention and to inform them of their right to opt out of receiving such communications;[177] and

[172] 74 Fed. Reg. 42740.
[173] 45 C.F.R. § 164.520.
[174] 78 Fed. Reg. at 5622 – 23 (proposed to be codified at 45 C.F.R. § 164.520(b)(1)(ii)(E)).
[175] 78 Fed. Reg. at 5623; 45 C.F.R. § 160.501.
[176] 78 Fed. Reg. at 5623; 45 C.F.R. § 164.520(b)(1)(iii)(A).
[177] 78 Fed. Reg. at 5623; 45 C.F.R. § 164.520(b)(1)(iii)(B).

- Require a statement explaining that a health care provider must honor an individual's request to restrict disclosure of protected health information to a health plan if the disclosure is for payment or health care operations and the information pertains solely to a health care item or service for which the individual has paid out of pocket in full, as provided in Section 164.522.[178]

HHS requested comments on whether the Privacy Rule should require a specific statement regarding the new legal duty for covered entities under the Breach Notification Rule and on ways to inform individuals in a timely manner of these material revisions to a covered entity's NPP[179] without unduly burdening health plans.[180]

Key Provisions of the Final Rule

HHS adopts all of the proposed amendments described above, with the exception of the proposed amendment regarding subsidized treatment communications.[181] Because the Final Rule treats subsidized treatment communications as marketing communications requiring an authorization, the only individuals who will receive these communications from a covered entity are those who affirmatively opt-in to do so.[182]

The Final Rule further modifies this section to require covered entities to include a specific statement in their NPP informing affected individuals of their right to be notified following a breach of unsecured protected health information (i.e., the Breach Notification Rule).[183] HHS disagreed with those commenters who believed that such a statement would cause individuals unnecessary concern or create unfounded fear that covered entities cannot appropriately secure health information. It clarifies that this requirement can be sufficiently met with a simple statement that an individual has a right to or will receive notifications of breaches of his or her unsecured protected health information. Covered entities that wish to include more detailed information are permitted to do so.[184]

In addition, the Final Rule sets forth new notification requirements related to material changes to NPPs. A health plan that posts its NPP on its web site is now required to: (1) prominently post the material change or its revised notice on its web site by the effective date of the material change to the notice (e.g., the compliance date of the Final Rule); and (2) provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan, such as at the beginning of the plan year or during the open enrollment period.[185]

---

[178] 78 Fed. Reg. at 5623; 45 C.F.R. § 164.520(b)(1)(iv)(A), 164.522(a)(1).
[179] 45 C.F.R. § 164.520(b)(3), requires prompt revision and distribution of NPPs to individuals when material changes are made.
[180] 78 Fed. Reg. at 5623.
[181] 78 Fed. Reg. at 5624; 45 C.F.R. § 164.520(b). (note that it does not codify the changes proposed at 45 C.F.R. § 164.520(b)(1)(iii)(A)).
[182] 78 Fed. Reg. at 5624.
[183] 78 Fed. Reg. at 5624; 45 C.F.R. § 164.520(b)(1)(v)(A).
[184] 78 Fed. Reg. at 5624 – 25.
[185] 78 Fed. Reg. at 5625; 45 C.F.R. § 164.520(c)(1)(v)(A).

Health plans that do not have customer service web sites are now required to provide the revised NPP, or information about the material change and how to obtain the revised notice, to individuals covered by the plan within 60 days of the material revision to the NPP.[186]

HHS notes that health plans and covered entities should provide both paper- and web-based notices in a way that is effective and accessible to all beneficiaries. Covered entities required to comply with Section 504 of the Rehabilitation Act or with the Americans with Disabilities Act must take any necessary steps to ensure that communication with individuals with disabilities is effective, such as making the revised NPP available in alternative formats like Braille, large print, or audio. HHS also notes that covered entities obligated to comply with Title VI of the Civil Rights Act of 1964 must take reasonable steps to ensure meaningful access for Limited English Proficient persons to the services of the covered entity, such as translating the NPP into frequently encountered languages.[187]

Summary of Relevant Comments and HHS Response

Several commenters expressed support for the requirement that the NPP include a statement about the uses and disclosures that require authorization.[188] Other commenters opposed this requirement, stating that because not all uses and disclosures will apply to every individual, the statement would cause confusion and unnecessary concern, and argued that listing all of the situations requiring authorization would be costly. HHS did not agree with these concerns, noting that the Final Rule does not require the NPP to include a list of all situations requiring authorization. HHS also clarified that covered entities that do not record or maintain psychotherapy notes are not required to include a statement in their NPPs about the authorization requirement for uses and disclosures of psychotherapy notes.[189]

HHS disagreed with the commenters who believed that the modifications to Section 164.520 do not constitute material changes to privacy practices requiring the distribution of revised NPPs. A few commenters expressed concern regarding the cost burden associated with revising and distributing new NPPs. However, HHS maintained its position that these modifications are significant and important to ensure that individuals are aware of the HITECH Act changes that affect privacy protections and individual rights regarding protected health information. HHS believes that the distribution requirements under the Final Rule reflect the appropriate balance between the rights of individuals to be informed of their privacy rights and the burden on health plans and covered entities to provide revised NPPs.[190]

Analysis

[186] 78 Fed. Reg. at 5625; 45 C.F.R. § 164.520(c)(1)(v)(B).
[187] 78 Fed. Reg. at 5625.
[188] 78 Fed. Reg. at 5623.
[189] 78 Fed. Reg. at 5624.
[190] 78 Fed. Reg. at 5625.

Several modifications have been made to the NPP requirements under Section 164.520 that will require covered entities and health plans to distribute and make available revised NPPs. HHS acknowledges that there is no "one size fits all" approach to meeting these new requirements and has attempted to give covered entities and health plans enough flexibility to determine how best to draft and prepare their NPPs based on their own circumstances. Although meeting these requirements will create some additional costs and burdens, HHS does not believe that they will be overly costly, burdensome, or unworkable.

45 C.F.R. § 164.522(a): Right to Request a Restriction of Uses and Disclosures

Relevant Statutory Provisions

Section 13405(a) of the HITECH Act requires a covered entity to comply with an individual's request to restrict the disclosure of his or her protected health information (unless the disclosure is otherwise required by law), if the disclosure is to a health plan for purposes of payment, treatment or health care operations, and the relevant information pertains solely to a health care item or service for which the provider has been paid out of pocket in full.[191]

Key Provisions of the Proposed Rule

Section 164.522(a) of the Privacy Rule requires a covered entity to allow an individual to request that the covered entity restrict uses or disclosures of the individual's protected health information for treatment, payment and health care operations purposes.[192] Covered entities were not required to agree to such requests. The Proposed Rule implements HITECH Section 13405(a) by modifying this section to require a covered entity to agree to such a request if the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law and the protected health information pertains solely to a health care item or service for which the individual (or person other than a health plan on behalf of the individual) has paid the covered entity in full.[193]

The Proposed Rule clarified that in cases where an individual has requested a restriction of disclosure to a health plan in the above the circumstances, a covered entity is also prohibited from making such disclosure to a business associate of the health plan.[194] The Rule proposed conforming modifications to the provisions regarding terminating

[191] HITECH Act, § 13405(a).
[192] 45 C.F.R. § 164.522(a)(1)(i)(A).
[193] 78 Fed. Reg. at 5626; 45 C.F.R. § 164.522(a)(1)(vi).
[194] 78 Fed. Reg. at 5626.

restrictions[195] and documentations of restrictions,[196] and to make clear that a covered entity may not unilaterally terminate a required restriction to a health plan.[197]

The Proposed Rule noted that it interpreted HITECH Section 13405(a) to give an individual discretion as to which items or services he or she wishes to pay for out of pocket and restrict; thus, a covered entity would not be permitted to require an individual to restrict disclosures of protected health information to a health plan regarding all health care, if the individual only wishes to restrict disclosure about certain health care items or services.

The Proposed Rule requested comment on the types of treatment interactions between individuals and covered entities that would make implementing a restriction more difficult and on the types of disclosures that may fall under the "required by law" exception. Comments were sought on whether covered health care providers who know of a restriction should notify other "downstream" providers of the restriction, including pharmacies, and if technology could facilitate such notification. Given HHS' understanding that most current HMO provider contracts prohibit the provider from accepting payment in full from the individual for the treatment provided, the Proposed Rule requested comment on how this modified provision would function with respect to HMOs.[198]

The Proposed Rule clarified that if an individual's out of pocket payment is not honored, the covered entity is not obligated to continue to abide by the requested restriction. HHS sought comment on the scope and extent of the expectation that in such cases, the covered entity must take reasonable steps to secure payment from the individual. The Rule also noted that an individual (or someone on behalf of an individual) paying out-of-pocket for a health care item or service should not expect that this payment would count towards the individual's out-of-pocket threshold with respect to his or her health plan benefits.[199]

Key Provisions of the Final Rule

The Final Rule adopts the proposed changes to Section 164.522.[200] A provider who discloses restricted information is in violation of the Privacy Rule and HITECH Act, and may face criminal penalties, civil monetary penalties, or corrective action.[201]The Final Rule clarifies the process by which a restriction can occur with respect to only one of several health care items or services provided in a single patient encounter, particularly where unbundling the services for purposes of billing a health plan is prohibited or more costly. HHS expects providers to counsel patients on the provider's ability to unbundle

[195] 78 Fed. Reg. at 5626; 45 C.F.R. § 164.522(a)(2).
[196] 78 Fed. Reg. at 5626; 45 C.F.R. § 164.522(a)(3).
[197] 78 Fed. Reg. at 5626.
[198] 78 Fed. Reg. at 5626.
[199] 78 Fed. Reg. at 5626.
[200] 78 Fed. Reg. at 5626; 45 C.F.R. § 164.522(a).
[201] 78 Fed. Reg. at 5630.

services and the impact of doing so; if the individual still desires a restriction after such counseling, and the provider is able to unbundle the item or service, the provider should do so. If a provider cannot unbundle the item or service, the provider should inform the individual and allow him or her to pay out of pocket for the entire bundle of services.[202]

The Final Rule maintains the approach to restrictions and follow-up care as discussed in the Proposed Rule. A provider may disclose previously restricted information to a health plan in order to have follow up care deemed medically necessary or appropriate, if disclosing such information is consistent with the provider's minimum necessary policies and procedures and the individual did not request a restriction with regard to the follow up treatment.[203]

In terms of business associates, the Final Rule clarifies that a provider who is prohibited from disclosing protected health information to a health plan may not disclose the information to the plan's business associate, but may disclose such information to its own business associates for the provider's own purposes.[204]

Summary of Relevant Comments and HHS Response

Comments were generally in support of the proposed modifications to Section 164.522(a) as an important right for health care consumers. However, there were also many concerns about the new requirements, including how to operationalize a restriction, the possibility of having to create separate records, and how to keep information restricted during health plan audits.[205] HHS clarified that providers need not keep separate medical records, but suggested that providers employ some way of flagging protected health information that has been restricted to ensure that this information is not inadvertently shared with the health plan. HHS noted that covered entities should already have mechanisms in place to appropriately limit the protected health information that is disclosed to a health plan and should be familiar with their application.[206]

There was support for the exception permitting disclosures that are required by law, but commenters sought clarification on how the modified provision would affect providers' existing legal obligations. HHS responded that disclosures that are otherwise required by law remain permissible.[207] If a provider is required by state or other law to submit a claim to a health plan for a covered service provided to the individual, and there is no exception or procedure for individuals wishing to pay out-of-pocket for the service, then disclosure of protected health information related to the covered service is required by law and is an exception to an individual's right to request a restriction.[208]

---

[202] 78 Fed. Reg. at 5630.
[203] 78 Fed. Reg. at 5630.
[204] 78 Fed. Reg. at 5630.
[205] 78 Fed. Reg. at 5627.
[206] 78 Fed. Reg. at 5628.
[207] 78 Fed. Reg. at 5628; 45 C.F.R. § 164.103.
[208] 78 Fed. Reg. at 5628 (note the discussion of an available exception for this situation with respect to Medicare).

Most commenters believed that it is an individual's obligation and not the provider's to inform downstream health care providers of a requested restriction.[209] Commenters were generally unaware of any system that would alert a downstream provider (such as a pharmacy) of restrictions electronically, and argued that it would be costly, burdensome, and unworkable for a provider to attempt to notify all subsequent providers of an individual's restriction request. HHS recognized the lack of automated technologies necessary to support notification of downstream providers, and thus the impracticality of instituting a notification requirement. HHS encouraged providers to assist individuals in alerting downstream providers of the requested restriction, but the Final Rule makes clear that it is the patient's obligation to notify downstream providers of a restriction request.[210]

There was support for the suggestion that HMO patients would have to use out-of-network providers to ensure that the restricted information would not be disclosed to the HMO, as many state laws and provider contracts prohibit providers from receiving a cash payment in excess of the patient's cost sharing amount. The Final Rule clarifies that a provider operating within an HMO context should abide by a patient's requested restriction unless doing so would be contrary to State or other law, and notes that HHS does not consider a contractual requirement to submit a claim or otherwise disclose protected health information to an HMO to exempt the provider from obligations under this provision.[211]

There was general support for permitting a restriction to apply when a third party (other than a health plan) pays for the individual's care. Most commenters supported not having to abide by a restriction if a patient's payment does not go through, and a few commenters suggested that a covered entity should include information in its notice of privacy practices to this effect.[212] This provision prompted concerns regarding the ability of the provider to get reimbursed by the health plan for services following an individual's inability to pay.[213] HHS noted that a provider may choose to require payment in full at the time of the request for a restriction to avoid payment issues altogether.[214] Several comments sought clarification on what constitutes a "reasonable effort" to obtain payment from an individual.[215] HHS declined to prescribe the efforts a health care provider must make and leaves it up to the provider's policies and individual circumstances.[216]

Commenters generally supported the idea that if an individual does not request a restriction and pay out of pocket for follow up care, the covered entity may disclose the protected health information necessary to obtain payment from the health plan for such

[209] 78 Fed. Reg. at 5627.
[210] 78 Fed. Reg. at 5629.
[211] 78 Fed. Reg. at 5629.
[212] 78 Fed. Reg. at 5627.
[213] 78 Fed. Reg. at 5628.
[214] 78 Fed. Reg. at 5630.
[215] 78 Fed. Reg. at 5628.
[216] 78 Fed. Reg. at 5629.

follow up care. Many commenters supported providers counseling patients on the consequences of not restricting follow up care, while others were concerned with how a provider would know such counseling was needed.[217]

Analysis

None.

45 C.F.R. § 164.524 – Access of Individuals to Protected Health Information

Relevant Statutory Provisions

Section 13405(e)(1) of the HITECH Act provides that when a covered entity uses or maintains an electronic health record[218] with respect to protected health information of an individual, the individual shall have a right to obtain from the covered entity or direct the covered entity to transmit to a designee, a copy of such information in an electronic format.[219]

Section 246(c) of HIPAA gives HHS regulatory authority to promulgate rules governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions governed by HIPAA.[220]

Key Provisions of the Proposed Rule

HHS proposed to expand the rights of individuals to access their individually identifiable health information by applying the right of access to all protected health information maintained in one or more designated record sets electronically, regardless of whether the designate record set is an electronic health record.[221] Amendments pertaining to each provision are discussed in further detail below.

Key Provisions of the Final Rule

Adopted as proposed.[222]

Summary of Relevant Comments and HHS Response

[217] 78 Fed. Reg. at 5628.
[218] HITECH Act, § 13400(5) defining an electronic health record as, "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff."
[219] HITECH Act, § 13405(e)(1).
[220] HIPAA, §264(c).
[221] 78 Fed. Reg. at 5631; HITECH Act § 13405(e).
[222] 78 Fed. Reg. at 5631; 45 C.F.R. § 164.524(c)(2)(ii).

Most commenters were opposed to expanding the scope of access to include all electronic designated record sets, favoring limiting the requirement to electronic health records as described in HITECH. HHS responded that the extended electronic right of access is important for individuals as covered entities increasingly transition from paper to electronic records.[223] While commenters sought clarification on what constitutes an electronic health record, HHS declined the need to further define the term, as the Final Rule gives individual access to protected health information maintained in an electronic designated data set, not just an electronic health record.[224]

Several commenters also sought clarification on how the new access requirements would apply to business associates. HHS clarified that the extent to which a business associate is involved in fulfilling a covered entity's obligation to provide an individual electronic access to their records is to be governed by the business associate agreement between the covered entity and business associate. Therefore, if a business associate is not required by its agreement with the covered entity to provide direct access to records, the Final Rule does not impose a separate requirement on business associates to do so.[225]

45 C.F.R. § 164.524(c)(2) –Form and Format

Relevant Statutory Provisions

The HITECH Act expands the requirement that a covered entity must provide an individual access to his or her protected health information in the form or format requested by the individual, by requiring a covered entity that uses or maintains an electronic health record to provide the individual with a copy of the information in an electronic format.[226]

HHS also has broader regulatory authority under Section 246(c) of HIPAA to implement the statutory provision above.[227]

Key Provisions of the Proposed Rule

HHS proposed an amendment to Section164.524(c)(2) stating that when an individual requests access to protected that is maintained electronically in a designated record set, the covered entity must give the individual access in the electronic form or format that

[223] 78 Fed. Reg. at 5631.
[224] 78 Fed. Reg. at 5631-32.
[225] 78 Fed. Reg. at 5632.
[226] 78 Fed. Reg. at 5632; 45 C.F.R. § 164.524(c)(2); HITECH Act § 13405(e).
[227] HIPAA, § 246(c).

the individual requests. If the protected health information is not readily producible in the electronic form or format that the individual requested, the entity must give the individual access to the protected health information in an alternative, readable electronic form or format agreed to by the entity and the individual.[228]

Key Provisions of the Final Rule

Adopted as proposed.[229]

Summary of Relevant Comments and HHS Response

Many comments requested clarification on permitted methods for offering protected health information on electronic media. Several comments reflected the need for flexibility for covered entities to determine available electronic formats.[230] In the Final Rule, HHS noted that the availability of a readable electronic form or format will vary and so covered entities have flexibility in determining which types of electronic formats are available.[231] HHS also noted that covered entities are not required to purchase new software or systems in order to accommodate a specific request, provided the entity is able to provide some form of electronic copy.[232] If an individual declines to accept any of the entity's readily producible electronic formats, a covered entity must provide a hard copy as an option to fulfill the access request.[233]

Several covered entities commented on the form of request for an individual to access his or her electronic protected health information. Some commenters opposed a request that was required to be written and signed.[234] HHS clarified that the access request does not have to be in writing, but may be required to be in writing by the covered entity as long as the entity informs the individual of this requirement. Therefore, under the Final Rule, covered entities may require requests to be in writing, or allow individuals to provide electronic documents and signatures to satisfy the written document requirement. However, HHS noted that a covered entity may also accept an individual's oral request for an electronic copy of his or her protected health information.[235]

Several commenters questioned what content must be provided in response to an electronic access request. HHS responded that just as is currently required for access

[228] 78 Fed. Reg. at 5631; HITECH Act § 13405(e); 45 C.F.R. § 164.524(c)(2).
[229] 78 Fed. Reg. at 5633; 45 C.F.R. § 164.524(c)(2)(ii).
[230] 78 Fed. Reg, at 5632.
[231] 78 Fed. Reg, at 5633.
[232] 78 Fed. Reg. at 5633.
[233] 78 Fed. Reg. at 5633.
[234] 78 Fed. Reg. at 5633.
[235] 78 Fed. Reg. 5633;

requests to protected health information stored in hard copy, covered entities must provide an electronic copy of all protected health information about the individual held in an electronically maintained designated record set at the time the request is fulfilled, unless otherwise restricted, including images or data electronically linked to the designated record set. The individual may request only a portion of the protected health information, in which case the covered entity need only provide the requested portion. Covered entities are not required to scan paper documents to provide electronic copies of records maintained in hard copy.[236]

Commenters raised several security-related concerns. HHS responded to these concerns by confirming that the new rule does not require entities to provide individuals with direct access to their systems,[237] and that entities need not comply with an individual's request to copy protected health information onto an external device if doing so would constitute an unacceptable security risk.[238] If an individual requests that protected health information be transmitted via unencrypted e-mail, the entity is only responsible for advising the individual of potential risks, and would thus not be responsible for unauthorized access to protected health information during transmission. HHS disagreed that this duty to warn would be unduly burdensome. [239]

Analysis

Throughout this section of the Final Rule, HHS reiterates that despite the amendments to Section 164.524, little has changed. The changes are only applicable to covered entities that maintain protected health information in electronic designated record sets and do not require entities to adopt new electronic systems. Further, the original access requirement already required covered entities to provide an electronic copy of protected health information, if the individual requested such format and the entity could readily produce such format. The only entities that must make changes are those that use electronic systems incapable of producing readable electronic copies. These entities will need to upgrade their systems in order to comply with the new requirements, but, as with all other entities, need not acquire the capacity to produce any and all electronic form or formats an individual could possibly request.

While commenters raised a number of concerns over the burdens of the new electronic access requirement, HHS's responses indicate that covered entities will retain significant discretion over implementation of the new requirement. Covered entities are under no obligation to assume a risk to the security of their systems in order to provide an

[236] 78 Fed. Reg. at 5633.
[237] 78 Fed. Reg. at 5631.
[238] 78 Fed. Reg. at 5634.
[239] 78 Fed. Reg. at 5634.

individual with requested access. However, system security concerns will not be a means by which an entity can avoid the electronic access requirement; an entity remains obligated to produce some kind of electronic copy unless an individual refuses to accept any of the electronic form or formats the entity is capable of readily and securely producing.

45 C.F.R. § 164.524(c)(3) – Third Parties

Relevant Statutory Provisions

Section 13405(e)(1) of the HITECH Act provides that an individual has the right to direct a covered entity to transmit an electronic copy of protected health information in an electronic health record directly to an entity or person designated by the individual, provided that such choice is clear, conspicuous, and specific.[240]

Further, HHS uses its authority under Section 264(c) under HIPAA to expand the language in the HITECH Act to also include the transfer of protected health information in either electronic or paper form.[241]

Key Provisions of the Proposed Rule

Section 164.524(c)(3) requires a covered entity to mail a copy (or summary or explanation) of protected health information if an individual requests.[242] HHS has previously interpreted this provision to require covered entities to mail a copy of the requested protected health information to an alternative (third party) address requested by the individual, as long as the request is clearly made by the individual and not a third party.[243]

The Proposed Rule expanded Section 164.524(c)(3) to provide that a covered entity must transmit a copy of the requested protected health information directly to another person designated by the individual, whether the protected health information is in electronic or paper form, if an individual requests. To satisfy HITECH's requirement that such a request be clear, conspicuous, and specific, the Proposed Rule would require the individual's request to be in writing, be signed by the individual, and clearly identify the designated person and where to send the copy of the protected health information. The Proposed Rule also allowed electronic documents and signatures to fulfill the written requirement of the Privacy Rule. The Proposed Rule also required a covered entity to

[240] 78 Fed. Reg. at 5634; HITECH Act, §13405(e)(1).
[241] HIPAA § 264(c).
[242] 45 C.F.R. § 164.524(c)(3).
[243] 78 Fed. Reg. at 5634.

implement reasonable policies and procedures to verify the identity of a requestor and implement safeguards to protect the information being used or disclosed.[244]

Key Provisions of the Final Rule

Adopted as proposed.[245]

Summary of Relevant Comments and HHS Response

Commenters sought clarification regarding transmission of an electronic copy of PHI to a third party designated by the individual and, in particular, whether an authorization is required prior to transmitting the requested information to a designated third party. HHS noted that in contrast to other access requests under this provision, where the entity has flexibility to accept written, oral, or electronic requests for access, requests for transmission to a third party must be made in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the protected health information.[246] This written request for protected health information is distinct from an authorization form, which contains many additional required statements and elements.[247]

Commenters also questioned whether they would be liable when making reasonable efforts to verify the identity of a third party recipient identified by an individual.[248] HHS clarified that covered entities may rely on the information provided in writing by the individual.[249]

Analysis

The new requirement for entities to transmit copies of protected health information to a third party designee is applicable whether the information is paper-based or stored electronically. Entities that do not currently require individual access requests in writing must nonetheless require and accept third-party transmission requests in writing, which could be burdensome. The Privacy Rule allows electronic documents to serve as written documents and permits e-signatures to satisfy signature requirements, so a covered entity could utilize an electronic system to accept third party transmission requests.

[244] 78 Fed. Reg. at 5634.
[245] 78 Fed. Reg. at 5634; 45 C.F.R. § 164.524(c)(3).
[246] 78 Fed. Reg. at 5634.
[247] 78 Fed. Reg. at 5635; 45 C.F.R. § 164.508(c).
[248] 78 Fed. Reg. at 5634.
[249] 78 Fed. Reg. at 5635.

While covered entities may rely on information from the individual identifying and designated a third party to whom the protected health information should be transmitted, covered entities must implement reasonable policies and procedures to verify the identity of any person who requests health information,[250] as well as reasonable safeguards to protect the information that is used or disclosed,[251] as required by other provisions of HIPAA.

45 C.F.R. § 164.524(c)(4) – Fees

Relevant Statutory Provisions

Section 13405(e)(2) of the HITECH Act provides that a covered entity may not charge more than its labor costs in responding to a request for an electronic copy of protected health information from an electronic health record.[252]

Key Provisions of the Proposed Rule

Section 164.524(c)(4) permits a covered entity to impose a reasonable, cost-based fee for producing a copy of requested protected health information (or summaries/explanations of protected health information if an individual agrees to this alternative).[253] This fee was limited to applicable and actual costs of: copying, including the supplies for and labor of copying; postage for mailing the copy; and preparation of the explanation or summary of the protected health information.

In reconciling the fee-related provisions in the Privacy Rule and the HITECH Act, the Proposed Rule amends Section 164.524(c)(4) to separately identify the labor costs associated with copying protected health information as one factor that may be included in the reasonable, cost-based fee.[254] The Proposed Rule retained all prior interpretations of labor with respect to paper copies, specifically that the labor cost may not include the costs associated with searching for and retrieving the requested information. Additionally, the Proposed Rule asserted that a reasonable cost-based fee with respect to electronic copies includes costs attributable to the labor involved to review the access request and to produce the electronic copy. While the Proposed Rule failed to consider a "retrieval fee" reasonable, it invited the public to comment on compensable aspects of labor.[255]

[250] 78 Fed. Reg. at 5635;45 C.F.R. § 164.514(h).
[251] 78 Fed. Reg. at 5635;45 C.F.R. § 164.530(c).
[252] HITECH Act, § 13405(e)(2).
[253] 45 C.F.R. § 164.524(c)(4).
[254] 78 Fed. Reg. at 5635; 45 C.F.R. § 164.524(c)(4)(i)).
[255] 78 Fed. Reg. at 5635.

The Proposed Rule further amended Section 164.524(c)(4) to provide separately for the cost of supplies for creating a paper copy or for the cost of portable electronic media (provided by the entity and requested by the individual) onto which electronically stored protected health information is copied.[256] HHS noted that a covered entity could charge a reasonable, cost-based fee for the electronic media provided as long as it was requested or agreed to by the individual. However, HHS did not change the provision permitting a covered entity to charge for postage for mailing a copy, but clarified that its interpretation of this provision would permit a covered entity to charge for postage if an individual requests that the entity transmit portable media containing an electronic copy through the mail.[257]

Key Provisions of the Final Rule

Adopted as proposed.[258]

Summary of Relevant Comments and HHS Response

Commenters were generally supportive of the inclusion of labor and, in some cases, supply costs to support the electronic access requirement. Commenters suggested a number of additional costs that should be permitted in the fees, including those associated with labor and retrieval.[259] In response, HHS clarified that labor costs can include skilled technical staff time spent to create and copy the electronic file, or time spent preparing an explanation or summary of the protected health information, if appropriate. Although HHS acknowledged commenters' assertions that the cost related to searching for and retrieving electronic protected health information in response to requests would not be negligible, it clarified that a covered entity may not charge a retrieval fee, whether it is a standard retrieval fee or one based on actual retrieval costs.[260]

Commenters also suggested inclusion of costs associated with materials and labor.[261] HHS noted that covered entities are not required to adopt or purchase new technology or systems to comply with specific format requests, and thus the cost of obtaining such new technologies or maintaining new systems may not be included in the fee.[262]

[256] 78 Fed. Reg. at 5635;45 C.F.R. § 164.524(c)(4)(ii).
[257] 78 Fed. Reg. at 5635;45 C.F.R. § 164.524(c)(4)(iii).
[258] 78 Fed. Reg. at 5635 – 636;45 C.F.R. § 164.524(c)(4).
[259] 78 Fed. Reg. at 5635.
[260] 78 Fed. Reg. at 5636.
[261] 78 Fed. Reg. at 5635.
[262] 78 Fed. Reg. at 5636.

In response to questions about state law limitations on fees for copying protected health information, HHS noted that copying fees must be both reasonable and cost-based and state laws are relevant to determine whether a fee is reasonable. Entities may only charge the actual amount incurred for copying, not to exceed the state's limit, even if the actual charge exceeds the state's limit.[263]

Analysis

HITECH permits only the inclusion of labor costs in the charge for electronic copies, thus excluding charges for supplies such as hardware or software used to generate electronic copies. This is in contrast to the permissible supply charges for making hard copies, and covered entities should be mindful of the difference in allowable fees. The distinction is justified because an electronic copy exists independent of media and can be transmitted electronically without accruing ancillary supply costs. The Final Rule does allow a covered entity to charge a reasonable and cost-based fee for any external portable electronic media device (such as a blank CD or a USB flash drive) onto which an electronic copy is transferred, at an individual's request.

Furthermore, the Final Rule's prohibition on retrieval fees ensures that fee requirements for electronic access are consistent with those for hard copies, which does not allow for retrieval fees for locating paper records.

45 C.F.R. § 164.524(b) – Timeliness

Relevant Statutory Provisions

None.

Key Provisions of the Proposed Rule

Section 164.524(b)(2) requires covered entities to act on access requests within 30 days of receiving the request. If the protected health information was inaccessible to the covered entity on-site, the entity had 60 days to act on the request. If a covered entity is unable to act on the request within the applicable time period, the entity may take a one-time 30 day extension.[264]

[263] 78 Fed. Reg. at 5636.
[264] 45 C.F.R. § 164.524(b)(2).

The Proposed Rule requested comment on a number of issues related to the timeliness provisions in the Privacy Rule that were not amended by HITECH.[265] With the advent of electronic health record systems, HHS recognized that there is an expectation and capability that information can be provided instantaneously. Specifically, HHS noted that a single, common standard for time in which a covered entity must provide access to records was preferred.[266]

Key Provisions of the Final Rule

The Final Rule modifies Section 164.524(b)(2) of the Privacy Rule related to the timeliness requirements for right to access protected health information. The Final Rule retains the provision granting entities 30 days to respond to a request for access to protected health information[267] with a one-time 30 day extension of this deadline.[268] However, the Final Rule removes the provision giving covered entities up to 60 days to respond when the protected health information is inaccessible to the covered entity on-site.

Summary of relevant comments and HHS responses

Commenters generally did not support modification of the time frames for response. HHS disagreed and stated that limiting the time frame for responses to requests for access to 30 days for all covered entities is both appropriate and achievable, particularly given the availability of a one-time 30-day extension. HHS confirmed that the time period for responding to a request for access begins on the date of the request.[269]

Analysis

The amended timeliness requirements will impact all covered entities, regardless of whether they use paper-based or electronic systems. The shortened timeframe is a reflection of what HHS cites as the "increasing expectation and capacity to provide individuals with almost instantaneous electronic access to their protected health information through personal health records or similar electronic means." Although this may be true for electronic copies, the shortened timeframe applies to paper copies as well, which will disproportionately impact those entities that utilize paper-only systems, particularly those that store records off-site. HHS encourages covered entities to provide access earlier than the standard 30 day limit, and to take advantage of technologies that provide individuals with immediate access to their protected health information. This

[265] 78 Fed. Reg. 5636-37.
[266] 78 Fed. Reg. at 5636.
[267] 78 Fed. Reg. at 5637; 45 C.F.R. § 164.524(b)(2)(i).
[268] 78 Fed. Reg. at 5637; 45 C.F.R. § 164.524(b)(2)(ii).
[269] 78 Fed. Reg. at 5637.

language and the shortened timeframe hint at an underlying expectation for all covered entities to begin utilizing electronic systems.

Modifications to the Security Rule

45 C.F.R. §§ 164.308, 164.310, 164.312, 164.316 – Business Associates

Relevant Statutory Provisions

The HITECH Act requires the Security Rule's administrative, physician and technical safeguards and the Rule's policies and procedures apply to business associates in the same way they apply to covered entities.[270]

Key Provisions of the Proposed Rule

The Proposed Rule adds "business associate" to Subpart C to ensure that the provisions of the Security Rule also apply to business associates.[271]

Key Provisions of the Final Rule

HHS adopts the Proposed Rule's changes to extend direct liability for compliance with the Security Rule to business associates. Also, covered entities and business associates have flexibility to determine the type and nature of the security measures are needed based on the nature of the security risks posed by each specific entity. For smaller, less sophisticated business associates, HHS has included an estimate of compliance costs in its regulatory impact analysis.[272]

Summary of Relevant Comments and HHS Response

There were comments both in support of and opposed to requiring business associates to comply with the Security Rule. In response to those commenters against this provision, HHS stated that business associates and subcontractors already have security practices that would be required in place to be in compliance with the Security Rule.[273]

Analysis

Imposing direct liability on business associates is a tremendous change from the original Security Rule. Business associates will therefore be responsible for adopting appropriate security measures based on the nature of the security risks posed.

[270] HITECH Act, § 13401.
[271] 78 Fed. Reg. at 5589; 45 C.F.R. §§ 164.306, 164.308, 164.312, 164.314, 164.316.
[272] 78 Fed. Reg. at 5589.
[273] 78 Fed. Reg. at 5589.

45 C.F.R. § 164.308 -Administrative Safeguards

Relevant Statutory Provisions

None.

Key Provisions of the Proposed Rule

The Proposed Rule removed the exceptions regarding a business associate contract standard, as they were included as exceptions to the definition of "business associate." The Proposed Rule also clarified that covered entities are not required to obtain satisfactory assurances from a subcontractor, but that it is the duty of a business associate to do so. Additionally, the Proposed Rule removed a provision that holds a covered entity liable for violating assurances it provided as a business associate because the Security Rule now directly applies to business associates.[274]

Key Provisions of the Final Rule

Adopted as proposed.[275]

Summary of Relevant Comments and HHS Response

In response to one comment, the Final Rule expressly states that a covered entity is not required to enter into a business associate agreement with a subcontractor, but that this is the obligation of the business associate that has contracted with the subcontractor.[276]

Analysis

As noted above, the final rule modifies Section 164.308(b) to oblige business associates to enter into a contract with a subcontractor who is enlisted to perform duties involving the use or disclosure of protected health information, rather than the covered entity.

45 C.F.R. § 164.314 -Organizational Requirements

Relevant Statutory Provisions

In order to fully comply with Section 13401 of the HITECH Act, Section 164.314 must be modified to reflect that the Security Rule applies to business associates in the same way it applies to covered entities.[277] Section 164.308(b) requires that a covered entity's business associate agreement conform to the standards set forth under Section 164.314.[278] Therefore, under the HITECH Act, Section 164.314 must be revised to reflect its

[274] 78 Fed. Reg. at 5590; 45 C.F.R. § 164.308(b)(1) and (2).
[275] 78 Fed. Reg. at 5590.
[276] 78 Fed. Reg. at 5590.
[277] 78 Fed. Reg. at 5590; 45 C.F.R. § 164.308(b).
[278] 78 Fed. Reg. at 5590; 45 C.F.R. § 164.308(b).

applicability to agreements between business associates and subcontractors that create, transmit, receive or maintain protected health information.[279]

Key Provisions of the Proposed Rule

The Proposed Rule revised Section 164.314 to apply to agreements between business associates and subcontractors that create, receive maintain or transmit protected health information. The Proposed Rule also amended Section 164.314 to reflect that business associates agreements must require the business associate to comply with Security Rule, ensure that subcontractors protect the security of health information, and that the business associate reports to the covered entity any breach of unescorted health information. The Rule also added a provision requiring that the contract provisions also apply to arrangements between a business associate and subcontractor.[280]

Key Provisions of the Final Rule

Adopted as proposed.[281]

Summary of Relevant Comments and HHS Response

HHS did not receive substantive comments on the Proposed Rule. Some of the comments received addressed the compliance time for the new requirements, and exemption of subcontractors from compliance.[282] HHS declined to give subcontractors additional time to comply with the requirements of the Security Rule because the Rule already requires that the business associate agreements contain many of the security provisions. Some commenters also suggested that HHS exempt subcontractors from compliance with the Security Rule if they have met other requirements, but HHS disagreed with this assessment.[283]

Analysis

None.

Modifications to the Breach Notification Rule

45 C.F.R. § 164.402 – Definitions

Relevant Statutory Provisions

[279] 78 Fed. Reg. at 5590l 45 C.F.R. §§164.308(b), 164.314.
[280] 78 Fed. Reg. at 5590.
[281] 78 Fed. Reg. at 5591.
[282] 78 Fed. Reg. at 5591.
[283] 78 Fed. Reg. at 5591.

Section 13400(1)(A) of the HITECH Act defines "breach" as the "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.[284]

Section 13400(1)(B) of the HITECH Act provides two additional exceptions to the definition of "breach."[285]

Section 13402(h)(1)(A) of the HITECH Act defines "unsecured protected health information" as protected health information that is not secured by a technology or methodology specified by the Secretary of HHS.[286]

Key Provisions of the Proposed Rule

The Interim Final Rule defined "breach" as "the acquisition, access, use, or disclosure of protected health information in a way that violates the Privacy Rule, which compromises the security or privacy of the protected health information." The security or privacy of protected health information is compromised if there is a "significant risk of financial, reputational, or other harm to the individual." HHS refers to this as the "harm standard."[287] Covered entities and business associates must conduct a risk assessment to determine whether the disclosure or use will result in a significant risk of harm to an individual. The Interim Final Rules provided that the use and disclosure of limited data sets[288] that exclude birth dates and zip codes did not compromise security or privacy of protected health information; this narrow exception was included in the belief that it would very difficult to re-identify such information, thus posing a low level of risk of harm to an individual in the event of a breach.[289]

The Interim Final Rule excluded the following situations from the definition of breach: (1) the unintentional acquisition, access, or use of protected health information by a workforce member or person acting on behalf of a covered entity or business associate if it occurred in good faith and within the scope of the person's authority and further use or disclosure in violation of the Privacy Rule does not occur; (2) inadvertent disclosures by persons authorized to access protected health information to other authorized persons at the same covered entity, business associate or organized health care arrangement in which the covered entity participates; or (3) disclosures to unauthorized persons if the covered entity or business associate believes, in good faith, that the recipient cannot reasonably retain the protected health information.[290]

[284] HITECH Act, § 13400(1)(A).
[285] HITECH Act, § 13400(1)(B).
[286] HITECH Act, § 13402(h)(1)(A).
[287] 78 Fed. Reg. at 5639.
[288] *See* 45 C.F.R. § 164.514(e)(2).
[289] 78 Fed. Reg. at 5640.
[290] 78 Fed. Reg. at 5640.

The Interim Final Rule defined "unsecured protected health information" as protected health information "that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary."[291]

Key Provisions of the Final Rule

The Final Rule defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part [164] which compromises the security or privacy of the protected health information."[292]

The Final Rule adopts the exceptions to the definition of breach as proposed in the Interim Final Rule.[293]

The Final Rule adds to the definition of breach to clarify that an impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate demonstrates on the basis of a risk assessment that there is a low probability that the information has been compromised.[294] This change removes the risk of harm standard and also modifies the requirements for the risk assessment.[295] The risk assessment must include, at minimum, consideration of the following factors: (1) the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the protected health information or to whom the disclosure was made; (3) whether the protected health information was actually acquired or viewed; and (4) the extent to which the risk to the protected health information has been mitigated."[296] HHS intends to issue guidance to assist covered entities and business associates in performing risk assessments with respect to frequently occurring scenarios.[297]

The Final Rule also removes the exception for limited data sets that do not contain any dates of birth and zip codes; thus, a risk assessment must be performed following the impermissible use or disclosure of any limited data set.[298]

The Final Rule adopts the Interim Final Rule's proposed definition of "unsecured protected health information" but replaces the term "unauthorized individuals" with the

[291] 78 Fed. Reg. at 5647 (noting that, in accordance with HITECH § 13402(h)(2), the Secretary issued guidance in which she specified that only encryption and destruction, consistent with the National Institute of Standards and Technology guidelines renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals such that notification is not required in the event of a breach of such information. This guidance was published within the preamble of the Interim Final Rule and made available on the HHS website).
[292] 45 C.F.R. § 164.402, at "Breach."
[293] 78 Fed. Reg. at 5644; 45 C.F.R. § 164.402, at ¶ 1 of the definition of "Breach."
[294] 78 Fed. Reg. at 5641; 45 C.F.R. § 164.402, at ¶ 2 of the definition of "Breach."
[295] 78 Fed. Reg. at 5641.
[296] 78 Fed. Reg. at 5642; 45 C.F.R. § 164.402, at ¶ 2 of the definition of "Breach."
[297] 78 Fed. Reg. at 5643.
[298] 78 Fed. Reg. at 5644.

term "unauthorized persons," because the definition of "individual" at Section 164.103 is inconsistent with the meaning of this section.[299]

Summary of Relevant Comments and HHS Response

HHS received numerous comments regarding the definition of "breach." Some commenters urged HHS to adopt a "bright line standard" that would require breach notification for all impermissible uses and disclosures without any assessment of risk, as this method would increase transparency and ease the enforcement burden.[300] Other commenters argued that the Interim Final Rule's subjective harm standard would lead to inconsistent risk assessments and thus should be replaced with objective criteria.[301] HHS agreed with the latter comments and thus amended the rule to include an objective standard. In conducting a risk assessment under the modified rule, covered entities and business associates must now evaluate the nature and the extent of the protected health information involved, the unauthorized persons who accessed the information and the extent to which the risk to the information has been mitigated, in addition to investigating whether the protected health information was actually acquired or viewed.[302]

Analysis

None.

45 C.F.R. § 164.404(a) – Notification to Individuals: Standard

Relevant Statutory Provisions

Section 13402(a) of HITECH requires covered entities that hold, use, or disclose unsecured protected health information to provide notice to each affected individual upon discovering a breach of such information.[303]

Section 13402(c) of HITECH treats a breach as discovered by a covered entity or business associate on the first day such breach is known or reasonably should have been known to the covered entity or business associate (or to the covered entity or business associate's employee, officer, or other agent, other than the person committing the breach).[304]

Key Provisions of the Proposed Rule

The Interim Final Rule required covered entities, upon discovering a breach of unsecured protected health information, to notify every individual whose unsecured protected health

[299] 78 Fed. Reg. at 5647; 45 C.F.R. § 164.402, at the definition of "Unsecured protected health information."
[300] 78 Fed. Reg. at 5641.
[301] 78 Fed. Reg. at 5642.
[302] 78 Fed. Reg. at 5642 – 643.
[303] HITECH Act, § 13402(a).
[304] HITECH Act, § 13402(c).

information has been, or is reasonably believed to have been accessed, acquired, used, or disclosed as a result of such breach.[305]

The Rule implemented HITECH's discovery provision (with respect to a covered entity) by stating that a covered entity discovers a breach on the first day that the covered entity or its workforce member or agent knew of the breach or would have known of the breach by exercising reasonable diligence.[306]

Key Provisions of the Final Rule

Adopted as proposed.[307]

Summary of Relevant Comments and HHS Response

Several commenters argued that a breach should be treated as discovered only after management has been notified of the incident and that a covered entity should not be held responsible for knowing of a breach if an appropriately trained employee fails to inform the proper persons. HHS disagreed, noting that this interpretation would be inconsistent with the HITECH Act, as well as with the HIPAA Enforcement Rule and the federal common law of agency. Commenters also sought guidance regarding what it means to be "exercising reasonable diligence." HHS responded that the term "by exercising reasonable diligence" is defined in the Enforcement Rule as "the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances."[308] HHS further noted that the determination of whether a person acted with reasonable diligence is a fact-based determinationthat involves the consideration of factors such as whether a covered entity took reasonable steps to learn of breaches and whether there were indications of breaches that a person "seeking to satisfy the Rule" would have investigated under similar circumstances.[309]

Analysis

None.

45 C.F.R. § 164.404(b) – Timeliness of notification

Relevant Statutory Provisions

Section 13402(d) of HITECH requires covered entities notify individuals of a breach "without unreasonable delay," but no later than 60 [calendar] days after discovering the

[305] 78 Fed. Reg. at 5647; 45 C.F.R. § 164.404(a)(1).
[306] 78 Fed. Reg. at 5647; 45 C.F.R. § 164.404(a)(2).
[307] 78 Fed. Reg. at 5647; 45 C.F.R. § 164.404(a).
[308] 78 Fed. Reg. at 5647; 45 C.F.R. § 160.401.
[309] 78 Fed. Reg. at 5647.

breach. Covered entities and business associates have the burden of establishing their compliance with the timeliness requirement.[310]

Key Provisions of the Proposed Rule

The Interim Final Rule adopted the HITECH provision regarding timeliness without modification.[311] The Rule noted that the time period for breach notification begins when the incident is first known, even if the investigation is incomplete and/or it is unclear whether the incident constitutes a breach. A covered entity must make notifications as soon as reasonably possible,[312] so in some cases, the 60 day outer limit may actually constitute an "unreasonable delay" in providing notification.

Key Provisions of the Final Rule

Adopted as proposed.[313]

Summary of Relevant Comments and HHS Response

HHS received comments requesting more time to provide notice, such as 120 days, and arguing that the timeframe should not begin to run until after a covered entity has completed its investigation and determined that a breach has actually occurred. HHS declined to extend or otherwise modify the timeframe for reporting, noting its belief that a longer time period could adversely impact affected individuals and the ability to mitigate adverse consequences. HHS also states that what constitutes "unreasonable" versus "unreasonable" delay is fact-specific, with many potentially relevant factors, such as the nature of the breach, the number of individuals affected, and the covered entity's resources.[314]

Analysis

None.

45 C.F.R. § 164.404(c) – Content of notification

Relevant Statutory Provisions

Section 13402(f) of HITECH details the required content of a breach notice, which includes: (1) a description of the breach; (2) a description of the types of information compromised (e.g., social security number, full names, birth dates, etc.); (3) information

[310] HITECH Act, § 13402(d)(1).
[311] 78 Fed. Reg. at 5648; 45 C.F.R. § 164.404(b).
[312] 78 Fed. Reg. at 5648, noting that "As soon as reasonably possible" is after the covered entity takes a reasonable time to investigate the breach in order to collect and develop the information required to be included in the notice to the individual. (
[313] 78 Fed. Reg. at 5648; 45 C.F.R. § 164.404(b).
[314] 78 Fed. Reg. at 5648.

on how individuals can protect themselves from harm that may result from the breach; (4) information on what the covered entity is doing to investigate the breach, mitigate losses, and to protect against any further breaches; and (5) contact procedures to ask questions or obtain further information.[315]

Key Provisions of the Proposed Rule

The Interim Final Rule incorporates HITECH's content requirements, with some modifications. The Rule requires that some information be included in the notices to the extent possible, such as: the date of the breach and the date of the discovery of the breach; whether full names, social security numbers, dates of birth, home addresses, account numbers, diagnoses or disability codes were involved in the breach;, and either a toll-free number, web site, or postal address for individuals to use in contacting the covered entity for questions/further information.[316] The Rule also replaced the term "mitigate losses" with "mitigate harm to individuals" to make clear that the notification should describe the steps the covered entity is taking to mitigate potential harm to individuals and that such harm is not limited to economic loss.[317]

The Rule required notices to be written in plain language. Covered entities with obligations under other laws (e.g., Title VI of the Civil Rights Act of 1964, Section 504 of the Rehabilitation Act, or the Americans with Disabilities Act) must ensure that all individuals have meaningful access to notices, such as by translating the notice into frequently encountered languages, or making the notice available in alternate formats, such as Braille or audio, as applicable.[318]

Key Provisions of the Final Rule

Adopted as proposed.[319]

Summary of Relevant Comments and HHS Response

Several commenters felt that the content requirements for breach notification were too vague.[320] HHS responded that the content provisions need to be sufficiently flexible to allow covered entities to tailor the breach notices based on the circumstances surrounding the breach and the entity.[321] Some commenters asked for notice templates and/or guidance about required content elements.[322] HHS expressed its intention to release notice templates and guidance in the future.[323]

[315] HITECH Act, § 13402(f).
[316] 78 Fed. Reg. at 5648; 45 C.F.R. § 164.404(c).
[317] 78 Fed. Reg. at 5648.
[318] 78 Fed. Reg. at 5648.
[319] 78 Fed. Reg. at 5649; 45 C.F.R. § 164.404(c).
[320] 78 Fed. Reg. at 5648.
[321] 78 Fed. Reg. at 5649.
[322] 78 Fed. Reg. at 5648.
[323] 78 Fed. Reg. at 5649.

Analysis

Covered entities have significant flexibility to craft the form of their breach notices.[324] However, the lack of uniform standards or guidance from HHS could result in covered entities providing too much or too little information about a breach which could, in turn, alarm or confuse individuals. Consequently, covered entities should carefully consider the impact of the notice on consumers when crafting the notice.

45 C.F.R. § 164.404(d) – Methods of Individual Notification

Relevant Statutory Provisions

Section 13402(e)(1) of HITECH requires that breach notification be sent by first class mail to an individual's last known address or, with an individual's consent, by email.[325] Notification may be provided in one or more mailings as the information becomes available. Covered entities must provide notice in a substitute form if insufficient or out-of-date contact makes it impossible to mail the notice directly to the individual.[326] If there is insufficient information for 10 or more individuals, substitute notice must either be a "conspicuous posting" on the covered entity's home page, or in major print or broadcast media in the geographic area where the affected individuals likely reside. If urgent notification is necessary due to the potential for "imminent misuse of unsecured protected health information," the covered entity may provide notice by telephone or other means.[327]

Key Provisions of the Proposed Rule

The Interim Final Rule adopted HITECH's methods for providing breach notification directly to an individual.[328] The Rule clarified that if the individual affected by the breach is a minor or otherwise lacks legal capacity, notice may be provided to the parent or personal representative of the individual to satisfy the notice requirement. If an affected individual is deceased, notice must be provided to either the individual's next of kin or personal representative, if the covered entity knows the individual is deceased and has the address of the next of kin or personal representative.[329]

The Rule adopted HITECH's requirements for providing substitute notification, with some modifications. If a covered entity lacks sufficient contact information to notify an individual, they may use a substitute notice that is "reasonably calculated to reach the individual."[330] If there is insufficient contact information for less than 10 individuals, substitute notice may be made "by an alternative form of written notice, telephone, or

[324] 78 Fed. Reg. at 5649.
[325] HITECH Act, §13402(e)(1)(A).
[326] HITECH Act, § 13402(e)(1)(B).
[327] HITECH Act, § 13402(e)(1)(C).
[328] 78 Fed. Reg. at 5649; 45 C.F.R. § 164.404(d)(1)(i).
[329] 78 Fed. Reg. at 5649; 45 C.F.R. § 164.404(d)(1)(ii).
[330] 78 Fed. Reg. at 5659; 45 C.F.R. § 164.404(d)(2).

other means."[331] If there is insufficient contact information for 10 or more individuals, substitute notice must be made through a conspicuous posting on the covered entity's home page (for a period of 90 days), or in a major print or broadcast media available in the geographic area where the affected individuals likely reside.[332] Both formats of substitute notice must include a toll free number that individuals may call to receive more information.[333] Substitute notice is unnecessary if the individual is deceased.[334]

The Interim Final Rule adopts HITECH's methods regarding urgent notification.[335]

Key Provisions of the Final Rule

Adopted as proposed.[336]

Summary of Relevant Comments and HHS Response

Several commenters questioned which entity has the responsibility for providing notifications to individuals when a breach occurs at or by a business associate. HHS clarified that the covered entity ultimately maintains the obligation to notify individuals of the breach, even if the business associate is also a covered entity. HHS did note that covered entities may delegate this responsibility to a business associate,[337] and suggests that covered entities and business associates should consider which entity is in the best position to provide notice to the individual, which will depend on the circumstances.[338]

Commenters expressed potential privacy concerns with mailing notice to a home address and suggested that covered entities be permitted to accommodate requests to notify individuals at alternative locations (or by alternative means).[339] In response, HHS noted that covered entities are not prohibited from sending a breach notice to an alternative address, or the individual's e-mail address, if the individual so requests, and are in fact required to accommodate any such reasonable request under the Privacy Rule.[340]

Analysis

If an individual refuses to receive written notice and will only accept communication orally or by telephone, covered health care providers may phone the individual to let him or her know that a written breach notification is available for pickup at the provider's office. If the individual refuses to pick up the notice, then the covered health care provider may provide all the information in the notice over the phone and document that

[331] 78 Fed. Reg. at 5649 – 650; 45 C.F.R. § 164.404(d)(2)(i).
[332] 78 Fed. Reg. at 5650; 45 C.F.R. § 164.404(d)(2)(ii)(A).
[333] 78 Fed. Reg. at 5650; 45 C.F.R. § 164.404(d)(2)(ii)(B).
[334] 78 Fed. Reg. at 5649;. 45 C.F.R. § 164.404(d)(2).
[335] 78 Fed. Reg. at 5650; 45 C.F.R. § 164.404(d)(3).
[336] 78 Fed. Reg. at 5650; 45 C.F.R. § 164.404(d).
[337] 78 Fed. Reg. at 5650.
[338] 78 Fed. Reg. at 5651.
[339] 78 Fed. Reg. at 5650.
[340] 78 Fed. Reg. at 5651; 45 C.F.R. § 164.522.

it has done so.[341] In this case, HHS will exercise enforcement discretion with respect to the "written notice" requirement.[342] Consequently, an individual's refusal to receive written notice may force covered health care providers to violate the written notice requirement. HHS plans to exercise enforcement discretion in such circumstances, but this stance does nothing to alleviate providers' liability concerns.[343]

When multiple covered entities participate in electronic health information exchange and there is a breach at the Health Information Organization (HIO), it may be difficult to determine what breached information is attributable to which covered entity's individuals. In these circumstances, the HIO can notify all potentially affected covered entities and those covered entities may delegate back to the HIO the responsibility of notifying affected individuals. Since the rules do not require covered entities to delegate notification responsibility in such situations, the potential to confuse individuals still exists. Covered entities and business associates should thus consider addressing delegation via contract.

45 C.F.R. § 164.406 – Notification to the Media

Relevant Statutory Provisions

Section 13402(e) of HITECH requires that covered entities provide notice through prominent media outlets, following the discovery of a breach affecting more than 500 individuals within a particular state or jurisdiction.[344]

Key Provisions of the Proposed Rule

The Interim Final Rule adopted HITECH's provision regarding notice to prominent media outlets serving a state or jurisdiction following discovery of a breach affecting more than 500 individuals within the state or jurisdiction.[345] The Rule further required covered entities to notify the media without unreasonable delay no later than 60 [calendar] days after the discovery of the breach.[346] Media notices must contain the same information as is required for individual notifications.[347]

Key Provisions of the Final Rule

Adopted as proposed, without the specific reference to American Samoa and the Northern Mariana Islands, which are now included in the definition of "State" at Section 160.103, as modified by these rules.[348]

---

[341] 78 Fed. Reg. at 5651.
[342] 78 Fed. Reg. at 5651;45 C.F.R. § 164.522.
[343] 78 Fed. Reg. at 5651.
[344] HITECH Act, § 13402(e)(2).
[345] 78 Fed. Reg. at 5652;45 C.F.R. § 164.406(a).
[346] 78 Fed. Reg. at 5652; 45 C.F.R. § 164.404(b).
[347] 78 Fed. Reg. at 5653; 45 C.F.R. §§ 164.404(c),164.406(c).
[348] 78 Fed. Reg. at 5653; 45 C.F.R. § 164.406.

Summary of Relevant Comments and HHS Response

HHS received a comment requesting clarification of the media's responsibility to publically report the information provided by a covered entity and another asking whether a covered entity could satisfy the requirements by posting a press release on its website. HHS clarified that the regulation does not require media outlets to report information from covered entities and emphasizes that posting a press release on the covered entity's website does not satisfy the notice requirement.[349]

Analysis

None.

45 C.F.R. § 164.408 – Notification to the Secretary

Relevant Statutory Provisions

Section 13408(e)(3) of HITECH requires covered entities to notify the Secretary of HHS immediately of breaches affecting at least 500 individuals; notification regarding breaches that affect less than 500 individuals may be logged and submitted annually.[350]

Section 13408(e)(4) of HITECH states that the Secretary must post a list on the HHS website identifying each covered entity that reports breaches affecting more than 500 individuals.[351]

Key Provisions of the Proposed Rule

The Interim Final Rules implemented HITECH's statutory provisions requiring covered entities to immediately notify the Secretary of breaches of unsecured protected health information affecting at least 500 individuals.[352] The Rule interpreted the term "immediately" to require notification be sent to the Secretary concurrently with the notification sent to the individual.[353] Covered entities must notify the Secretary of all discovered breaches involving more than 500 individuals, regardless of whether the breach involved more than 500 residents of a particular State or jurisdiction.[354]

The Interim Final Rules required covered entities to document breaches that affect fewer than 500 people and annually submit the information to the Secretary, in a form specified on the HHS website, within 60 [calendar] days of the end of the year for all breaches that occurred during the preceding calendar year.[355]

[349] 78 Fed. Reg. at 5653.
[350] HITECH Act, § 13402(e)(3).
[351] HITECH Act, § 13402(e)(4).
[352] 78 Fed. Reg. at 5653; 45 C.F.R. § 164.408.
[353] 78 Fed. Reg. at 5653; 45 C.F.R. § 164.404.
[354] 78 Fed. Reg. at 5653 – 654.
[355] 78 Fed. Reg. at 5654; 45 C.F.R. § 164.408(c).

The HHS web site will specify the manner in which all of these notifications must be provided.[356]

Key Provisions of the Final Rule

The Final Rules adopt the proposed requirements governing notification to the Secretary, with one modification. Under the Final Rule, covered entities must notify the Secretary of all breaches of unsecured protected health information affecting fewer than 500 individuals no later than 60 days after the end of the calendar year in which the breaches were discovered, not the year in which the breaches occurred.[357]

Summary of Relevant Comments and HHS Response

HHS received comments expressing concerns about providing notice to the Secretary in the year following the "occurrence" of a breach since it is possible that a covered entity or business associate will not "discover" a breach until well after it occurs. HHS recognized the likelihood of these situations and amended Section 164.408(c) accordingly." Comments also urged HHS to permit covered entities to log all breaches affecting fewer than 500 individuals and then submit that log. HHS recognized that submitting each breach individually through the online form is burdensome and is exploring alternative submission methods. [358]

Analysis

None.

45 C.F.R. § 164.410 – Notification by a Business Associate

Relevant Statutory Provisions

Section 13402(b) of HITECH requires a business associate of a covered entity that holds, uses, or discloses unsecured protected health information to notify the covered entity when it discovers a breach of such information.[359]

Key Provisions of the Proposed Rule

The Interim Final Rule required that a business associate notify the covered entity after the discovery of a breach of unsecured protected health information.[360] A breach is discovered on the day that the business associate, or its employee, officer, or agent, knew

[356] 78 Fed. Reg. at 5653, 5654.
[357] 78 Fed. Reg. at 5654; 45 C.F.R. §164.408.
[358] 78 Fed. Reg. at 5654.
[359] HITECH Act, § 13402(b).
[360] 78 Fed. Reg. at 5655; 45 C.F.R. § 164.410(a)(1).

of the breach or would have known of the breach by exercising reasonable diligence.[361] Notice must be provided to the covered entity without unreasonable delay and in no case later than 60 days after the breach is discovered.[362] To the extent possible, the business associate must identify the individuals whose information has been, or is reasonably believed to have been, compromised and must also provide any available information that covered entities are required to include in notices to individuals.[363] This information can be provided at the time the business associate notifies the covered entity of the breach, or promptly thereafter as information becomes available, even if it is after the 60-day notification period.[364]

Key Provisions of the Final Rule

The Final Rule adopts the proposed notification requirements for business associates, but makes one technical, non-substantive correction to the section.[365]

Summary of Relevant Comments and HHS Response

Section 164.404(a)(2) provides that covered entities discover a breach when their agent discovers it.[366] Thus, the discovery of a breach by a business associate that is an agent of a covered entity will automatically trigger the covered entity's breach notification obligations.[367] HHS received numerous comments expressing concern regarding the effect of this rule on covered entities. One commenter argued that if knowledge is imputed when the business associate- discovers a breach, a covered entity will not have sufficient time to meet the timeliness requirement for individual notice. Other commenters asked for guidance on when business associates are considered agents of covered entities. HHS recognized that there are many types of relationships that can develop between a covered entity and a business associate based upon the functions that the business associate performs. In light of these variations, HHS felt that the federal common law of agency and the approach taken in the Enforcement Rule for determining agency liability are the appropriate standards for determining whether a business associate is or is not an agent of a covered entity.[368]

Analysis

None.

45 C.F.R. § 164.412(a) – Law Enforcement Delay

Relevant Statutory Provisions

[361] 78 Fed. Reg. at 5655; 45 C.F.R. § 164.410(a)(2).
[362] 78 Fed. Reg. at 5655; 45 C.F.R. § 164.410(b).
[363] 78 Fed. Reg. at 5655 – 566; 45 C.F.R. § 164.410(c).
[364] 78 Fed. Reg. at 5656.
[365] 78 Fed. Reg. at 5656; 45 C.F.R. § 164.510.
[366] 45 C.F.R. § 164.404(a)(2).
[367] 78 Fed. Reg. at 5655.
[368] 78 Fed. Reg. at 5656.

Section 13402(g) of HITECH requires covered entities and business associates to delay notification, notice or posting as required under the breach notification rule if a law enforcement official determines that provision of such notification, notice, or posting would impede an investigation or threaten national security.[369]

Key Provisions of the Proposed Rule

The Interim Final Rule required covered entities and business associates to temporarily delay breach notification to an individual, the media (if applicable), a covered entity by a business associate, and to the Secretary, if instructed to do so by a law enforcement official.[370] If the official states in writing that a delay is necessary because notification would impede a criminal investigation or cause damage to national security, the delay must last as long as the official specifies.[371] If an official makes an oral request, the covered entity or business associate must document the request, including the identity of the requesting official, and delay notification no longer than 30 days from the date of the oral request, unless a written statement is provided during that time[372]

Key Provisions of the Final Rule

Adopted as proposed.[373]

Summary of Relevant Comments and HHS Response

None received.[374]

Analysis

None.

45 C.F.R. § 164.414 – Administrative Requirements and Burden of Proof

Relevant Statutory Provisions

None.

Key Provisions of the Proposed Rule

The Interim Final Rule required covered entities to comply with the administrative requirements in Section 164.530 regarding training, complaints, sanctions, retaliation,

[369] HITECH Act, § 13402(g).
[370] 78 Fed. Reg. at 5657; 45 C.F.R. § 164.412.
[371] 78 Fed. Reg. at 5657; 45 C.F.R. § 164.412(a).
[372] 78 Fed. Reg. at 5657; 45 C.F.R. § 164.412(b).
[373] 78 Fed. Reg. at 5657; 45 C.F.R. § 164.412.
[374] 78 Fed. Reg. at 5657.

waiver, and policies.[375] The Rule also required that following an impermissible use or disclosure under the Privacy Rule, covered entities and business associates have the burden of demonstrating that all required notifications were made and that an impermissible use or disclosure did not constitute a breach, as defined in Section 164.402.[376]

Key Provisions of the Final Rule

Adopted as proposed.[377]

Summary of Relevant Comments and HHS Response

One commenter requested that HHS include a presumption that a breach did not occur if a covered entity or business associate has implemented a breach notification policy, completed a risk assessment and documented that it followed its policy in reaching a conclusion that breach notification was unnecessary.[378] HHS declined to create this presumption, as HITECH specifically places the burden of proof on covered entities and business associates to demonstrate that all notifications were made as required. HHS emphasized the importance of documenting compliance with the breach notification requirements.[379]

Analysis

None.

Modifications to the Enforcement Rule

45 C.F.R. § 160.304 – Principles for Achieving Compliance; 45 C.F.R. § 160.306 – Complaints to the Secretary; 45 C.F.R. § 160.308 – Compliance Reviews; and 45 C.F.R. § 160.312 – Secretarial Action Regarding Complaints and Compliance Reviews

Relevant Statutory Provisions

Section 13410(a) of the HITECH Act requires HHS to formally investigate a complaint if a preliminary investigation of the facts indicates a possible violation due to willful neglect and to impose a civil money penalty for such a violation.[380]

Key Provisions of the Proposed Rule

[375] 78 Fed. Reg. at 5657; 45 C.F.R. § 164.414(a).
[376] 78 Fed. Reg. at 5657; 45 C.F.R. § 164.414(b).
[377] 78 Fed. Reg. at 5657; 45 C.F.R. § 164.414.
[378] 78 Fed. Reg. at 5657.
[379] 78 Fed. Reg. at 5658.
[380] 78 Fed. Reg. at 5578.

Section 160.304 requires the Secretary to attempt to obtain covered entities' cooperation, regarding compliance with the applicable administrative simplification provisions, "to the extent practicable."[381] The Secretary may also provide technical assistance to covered entities as they attempt to comply with such provisions.[382] The Proposed Rule sought to apply this section to business associates as well as covered entities[383] and to clarify that the Secretary would seek their cooperation "to the extent practicable *and consistent with the provisions of this subpart....*" (emphasis added). This revision would allow HHS to comply with the HITECH Act requirement that they impose penalties for violations that arise due to willful neglect without obtaining an entity's cooperation.[384]

Pursuant to Section 160.306 persons may file complaints with the Secretary if they believe that a covered entity is not complying with the administrative simplification provisions. Persons must file their complaint in accordance with various specifications (e.g., in writing, within 180 days of obtaining knowledge of the possible violation, etc.). The Secretary has discretion whether to investigate such complaints and may review a covered entity's policies, procedures, and practices while conducting the investigation. The Secretary must provide, in its initial communication with the covered entity, a description of the act or omission that originated the complaint.[385]

The Proposed Rule sought to amend Section 160.306 to implement Section 13410(a) of the HITECH Act by requiring the Secretary to investigate complaints of violations due to willful neglect. However, the Secretary would retain discretion to review all other violations.[386] HHS also proposed to apply the rule to business associates.[387]

The Proposed Rule sought to add a new paragraph at Section 160.308 to provide that the Secretary may conduct reviews to assess covered entities' compliance with the administrative simplification provisions.[388] Although the HITECH Act does not require the Secretary to conduct compliance reviews in cases of "willful neglect," HHS proposed that such a requirement "furthers Congress' intent to strengthen enforcement with respect to potential violations due to willful neglect and ensures that investigations…are handled in a consistent manner."[389] Consequently, the Proposed Rule required the Secretary to conduct a compliance review if "a preliminary review of the facts indicates a possible violation due to willful neglect," although the Secretary would continue to have discretion to conduct such reviews in all other circumstances.[390] HHS also proposed to apply the rule to business associates.[391]

---

[381] 45 C.F.R. § 160.304.
[382] 45 C.F.R. § 160.304.
[383] 78 Fed. Reg. at 5577.
[384] 78 Fed. Reg. at 5578.
[385] 45 C.F.R. § 160.306.
[386] 78 Fed. Reg. at 5578.
[387] 78 Fed. Reg. at 5577.
[388] 78 Fed. Reg. at 5578.
[389] 75 Fed. Reg. at 40876.
[390] 78 Fed. Reg. at 5578.
[391] 78 Fed. Reg. at 5577.

Under prior Section 160.312, when a review revealed a covered entity's noncompliance with an administrative simplification provision, the Secretary was required to try to resolve the matter through informal means (e.g., corrective action plan, demonstrated compliance, etc.). If the Secretary and covered entity did not achieve an informal resolution, then the Secretary was required to (1) inform the covered entity that an informal resolution was not possible and (2) give the covered entity 30 days to respond with defenses or mitigating factors.[392]

The Proposed Rule sought to give the Secretary discretion over whether or not to resolve violations through informal means. This change reflected the HITECH Act's mandate that the Secretary formally investigate and penalize violations attributable to "willful neglect." Additionally, the Proposed Rule sought to have the Secretary either give the covered entity notice of impending civil money penalties, as required by Section 160.420, or written notice that no further action would be taken.[393] HHS also proposed to apply the rule to business associates.[394]

Key Provisions of the Final Rule

Adopted as proposed.[395]

Summary of Relevant Comments and HHS Response

Commenters expressed concern about requiring the Secretary to conduct compliance reviews where not expressly required by statute and about the possibility of duplication between complaint investigations and compliance reviews. HHS responded that it is appropriate to strengthen enforcement and improve consistency in the handling of complaints and compliance reviews where willful neglect is indicated, emphasizing that HHS retains discretion where a preliminary review indicates less than willful neglect. HHS indicated that duplication is not a concern because compliance reviews are generally done where allegations of violation are discovered through a mechanism other than a complaint (such as a media report or another agency), and a compliance review is not required after investigation of a complaint is initiated.[396]

Commenters also requested clarification of what constitutes a "preliminary review of the facts" for purposes of identifying a possible violation due to willful neglect, with some commenters suggesting the review should go beyond the allegations asserted in the complaint. HHS explained that it will determine, on a case-by-case basis, if the preliminary review should be expanded and whether additional inquiries are necessary to determine whether willful neglect is indicated.[397]

[392] 45 C.F.R. § 160.312.
[393] 78 Fed. Reg. at 5578, 5690.
[394] 78 Fed. Reg. at 5577.
[395] 78 Fed. Reg. at 5578-79.
[396] 78 Fed. Reg. at 5578-79.
[397] 78 Fed. Reg. at 5579.

Analysis

These provisions strengthen the enforcement authority of HHS and ensure that all complaints or other indications of violations due to willful neglect are properly investigated.

45 C.F.R. § 160.310 – Responsibilities of Covered Entities and Business Associates

Relevant Statutory Provisions

None.

Key Provisions of the Proposed Rule

Section 160.310 requires covered entities to (1) maintain records regarding their compliance with the administrative simplification provisions; (2) provide the Secretary with copies of these records and compliance reports at the Secretary's direction; (3) cooperate with the Secretary's investigation; and (4) provide the Secretary with access to their "facilities, books, records, accounts, and other sources of information" relevant to the review. The Secretary may only access such information during normal business hours unless "exigent circumstances exist." If a third party that maintains relevant information refuses to provide the information, the covered entity must certify and describe their efforts to obtain such information. The Secretary may only disclose protected health information obtained during a review in relation to the review or as otherwise permitted by law.[398]

The Proposed Rule sought to permit the Secretary to disclose protected health information obtained during a review to other government entities for law enforcement purposes in accordance with Section 552a(b)(7) of the Privacy Act.[399,400] This change would allow the Secretary to release information to state attorneys general and the Federal Trade Commission, among others.[401] HHS also proposed to apply the rule to business associates.[402]

Key Provisions of the Final Rule

Adopted as proposed.[403]

Summary of Relevant Comments and HHS Response

[398] 45 C.F.R. § 160.310.
[399] 5 U.S.C. § 552a(b)(7).
[400] 78 Fed. Reg. at 5579.
[401] 78 Fed. Reg. at 5579.
[402] 78 Fed. Reg. at 5577.
[403] 78 Fed. Reg. at 5579.

There was one comment requesting clarification and transparency on collaboration and information sharing between federal regulators and between federal and state agencies. In response, HHS referred to its online information regarding coordination with the Department of Justice and the Federal Trade Commission for enforcement actions. With respect to coordination with states, HHS noted that it would coordinate with state attorneys general as necessary.[404]

Analysis

The modification expands the authority of HHS to disclose protected health information collected from covered entities during an investigation or compliance review to other federal and state agencies if permitted under the federal Privacy Act, even if the disclosure is not necessary for enforcing the HIPAA Rules or otherwise required by law.

45 C.F.R. § 160.401 – Definition of "Reasonable Cause"

Relevant Statutory Provisions

Section 13410(d) of the HITECH Act established four tiers of increasing liability for HIPAA violations based on the level of culpability of a covered entity using the terms "reasonable diligence," "reasonable cause," and "willful neglect" to describe such levels of culpability that correspond to increasing minimum penalties. The lowest penalty (first) tier applies where a covered entity or business associate did not know and, by exercising reasonable diligence, would not have known of the violation; the next higher (second) tier applies to violations due to reasonable cause and not willful neglect; the second highest (third) tier applies to violations due to willful neglect corrected in a certain period of time; and the highest (fourth) tier applies to willful neglect that is not corrected.[405] The HITECH Act did not amend the definition of the terms "reasonable diligence," "reasonable cause," and "willful neglect," which had been defined in the prior HIPAA Rules.[406]

Key Provisions of the Proposed Rule

In the Interim Final Rule, HHS moved the definitions of these three terms from the section pertaining to affirmative defenses (Section 160.410) to the section applying to the entirety of Subpart D (Section 160.401) and the imposition of civil monetary penalties.[407] The prior HIPAA Rules defined these terms as follows:

- "Reasonable diligence" refers to "the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances;"

[404] 78 Fed. Reg. at 5579.
[405] HITECH Act, § 13410(d).
[406] 78 Fed. Reg. at 5579-80.
[407] 74 Fed. Reg. at 56126.

- "Reasonable cause" refers to "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;" and
- "Willful neglect" refers to "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated." [408]

The Proposed Rule sought to modify the definition of "reasonable cause," but not the other two terms. HHS believed the modification was necessary to clarify the state of mind required for this category of violations in order to ensure that all violations were captured by one of the penalty tiers. Specifically, HHS proposed to change the definition of "reasonable cause" to "an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect."[409] HHS also proposed to apply the rule to business associates.[410]

Key Provisions of the Final Rule

Adopted as proposed.[411] In addition, HHS intends to make available on its website the examples and guidance for application of the three terms to distinguish among the tiers that were previously included in the Proposed Rule.[412]

Summary of Relevant Comments and HHS Response

Commenters expressed general support for the change.[413]

Analysis

None.

45 C.F.R. § 160.402 – Basis for a Civil Money Penalty

Relevant Statutory Provisions

HHS using its authority.

Key Provisions of the Proposed Rule

HHS proposed to apply the rule to business associates.[414] In addition, HHS proposed to remove the exception at Section 160.402(c) for covered entity liability for the acts of

[408] 45 C.F.R. § 160.401.
[409] 78 Fed. Reg. at 5580.
[410] 78 Fed. Reg. at 5577.
[411] 78 Fed. Reg. at 5580.
[412] 78 Fed. Reg. at 5580.
[413] 78 Fed. Reg. at 5580.

business associate agents and add a new paragraph (2) under Section 160.402(c) providing for a civil money penalty against a covered entity or business associate for the acts of its agents. This change ensures that covered entities remain liable for any HIPAA obligations they have contracted out to another party, but will not be liable if the business associate is not an agent (e.g., a subcontractor). The Proposed Rule tracks the language of the Social Security Act Section 1128A(l), which states that "a principal is liable for penalties . . . for the actions of the principal's agents acting within the scope of the agency."[415]

Key Provisions of the Final Rule

Adopted as proposed.[416]

Summary of Relevant Comments and HHS Response

Several commenters requested clarification on how the federal common law of agency would apply to business associate relationships under the Proposed Rule, expressing concern that the rule would add confusion and undue burden to such relationships. HHS responded that a covered entity is generally liable for acts of its agents under common law. Referencing the preamble to the Enforcement Rule, HHS clarified that federal common law was adopted to define and apply the terms "principal," "agent," and "scope of agency," since the statute is silent on those definitions. Noting that adopting federal common law would be appropriate to apply HIPAA uniformly nationwide, HHS explained the general principles that apply to an analysis of whether a business associate is an agent and list the factors that indicate the scope of agency. HHS stressed that the right or authority to control the business associate's conduct is the essential factor in determining whether an agency relationship exists (giving examples of when such a relationship is likely to be found), not the terms, statements, or labels given to the parties.[417]

One commenter suggested that any deviation from the terms of a business associate contract would place the action, by definition, outside the scope of agency. HHS disagreed, explaining that a business associate's conduct would be within the scope of agency when it occurs during the performance of the assigned work, regardless of whether the work is done correctly or carelessly, or in disregard of the covered entity's instructions.[418]

Analysis

While the HITECH Act made business associates directly liable for HIPAA violations, the regulation clarifies that where the business associate is acting as an agent of the

[414] 78 Fed. Reg. at 5577.
[415] 78 Fed. Reg. at 5580-81.
[416] 78 Fed. Reg. at 5581.
[417] 78 Fed. Reg. at 5581.
[418] 78 Fed. Reg. at 5582.

covered entity, such as when the covered entity delegates certain of its duties under HIPAA to a business associate, the covered entity still may be liable for violations.

45 C.F.R. § 160.404 – Amount of a Civil Monetary Penalty

Relevant Statutory Provisions

Section 13401(d) of the HITECH Act allows civil monetary penalties to be imposed on covered entities and business associates under a tiered liability structure, with increasing penalties for increasing levels of culpability.[419]

Key Provisions of the Proposed Rule

The Interim Final Rule implemented the new penalty scheme for violations occurring on or after February 18, 2009.[420] For such violations, the Secretary must impose penalties as follows: (1) if the covered entity did not know of the violation and would not have known of the violation even through the exercise of reasonable diligence, the penalty for each violation must be between $100 and $50,000 with a maximum total of $1.5 million in yearly liability for violations under the identical provision; (2) if the covered entity's violation "was due to reasonable cause," the penalty for each violation must be between $1,000 and $50,000 with a maximum total of $1.5 million in yearly liability for violations under the identical provision; (3) if the violation occurred "due to willful neglect," but the covered entity corrected the violation within 30 days of obtaining knowledge of the violation or the date by which they should have obtained such knowledge, the penalty for each violation must be between $10,000 and $50,000 with a maximum total of $1.5 million in yearly liability for violations under the identical provision; and (4) if the violation occurred "due to willful neglect," but was not corrected during the 30 day period, then the penalty for each violation must be at least $50,000 with a maximum total of $1.5 million in yearly liability for violations under the identical provision.[421]

HHS proposed to amend the rule so that business associates are subject to civil money penalties in the same manner as covered entities for violations that arise after February 18, 2009.[422] HHS will not automatically impose the maximum penalties, but will exercise its discretion to apply penalties based on factors such as the nature and extent of the violation and resulting harm.[423]

Key Provisions of the Final Rule

Adopted as proposed, including changes previously implemented in the Interim Final Rule.[424]

---

[419] 78 Fed. Reg. at 5582.
[420] 74 Fed. Reg. at 56126; 45 C.F.R. § 160.404.
[421] 78 Fed. Reg. at 5582-83.
[422] 78 Fed. Reg. at 5577.
[423] 78 Fed. Reg. at 5583.
[424] 78 Fed. Reg. at 5583.

Summary of Relevant Comments and HHS Response

Some comments expressed concern about the impact of the new penalty structure on covered entities, particularly smaller ones. Some argued that the maximum penalty amounts for each violation and for a calendar year, which are the same for all penalty tiers, are inconsistent with the HITECH Act's tiered liability structure. HHS responded that it would exercise its discretion on imposing penalties with consideration of the nature and extent of the violation and resulting harm, noting that relevant factors include the financial condition and size of the covered entity or business associate.[425]

Some commenters argued that the Secretary should not be allowed to impose the maximum penalty amounts for the two lowest tiers (i.e., no knowledge of violations and violations due to reasonable cause). HHS responded that in those cases, the entity may establish that an affirmative defense applies under Section 160.410, where the entity corrects the violation within 30 days from the date the entity knew or, with the exercise of reasonable care, should have known of the violation. HHS also emphasized that the Secretary has discretion to waive penalties in whole or in part under Section 160.412, to the extent that payment of the penalty would be excessive relative to the violation, and also has authority under 42 U.S.C. § 1320a-7a(f) to settle any issue or case or to compromise the amount of any civil money penalty for violation of the HIPAA Rules.[426] Finally, HHS noted that entities may always appeal any penalty to an administrative law judge.[427]

Some commenters requested clarification as to how violations will be counted for purposes of calculating penalties. For example, would the loss of unsecured electronic media containing several hundred records be counted as a single violation? HHS responded that how violations are counted will depend on the circumstances surrounding the noncompliance, but that in general, the number of identical violations of the Privacy Rule will be counted by the number of individuals affected.[428]

Analysis

HHS declined to restrict its discretion in enforcement and the imposition of penalties, but gave some additional guidance regarding relevant factors that will influence enforcement and penalty decisions.

45 C.F.R. § 160.408 – Factors Considered in Determining the Amount of a Civil Money Penalty

Relevant Statutory Provisions

[425] 78 Fed. Reg. at 5583.
[426] 78 Fed. Reg. at 5583-84.
[427] 45 C.F.R. § 160.504
[428] 78 Fed. Reg. at 5584.

Section 13410(d) of the HITECH Act requires HHS to base determinations of penalty amounts on the nature and extent of the violation and the nature and extent of the harm resulting from such violation, but does not modify the section of the law requiring application of the above factors.[429]

Key Provisions of the Proposed Rule

When determining the amount of a civil money penalty, the Secretary may consider the following factors: (1) "the nature of the violation, in light of the purpose of the rule violated;" (2) "the circumstances, including the consequences of the violation…" (e.g., the time period of the violation, the occurrence of physical or financial harm, and whether the violation affected access to health care); (3) the covered entity's degree of culpability, including its intent and amount of control over the violation; (4) the covered entity's compliance history, including the similarity of the current violation to past violations, its response to prior violations, its response to the Secretary's technical assistance, and its response to prior complaints; (5) the covered entity's financial situation, including whether its financial status affected its compliance efforts, whether civil money penalties would impact its ability to provide care, and the size of the entity; and (6) "such other matters as justice may require."[430] The Secretary has discretion to consider additional circumstances.[431]

HHS proposed to amend the first two factors so that the Secretary must consider: (1) "the nature and extent of the violation," including the number of persons affected by the violation and the time period of the violation; and (2) "the nature and extent of the harm resulting from the violation," including whether the violation caused physical, financial, or reputational harm or affected individuals' access to care.[432] HHS also proposed to remove the factor regarding a covered entity's culpability because that factor is now incorporated in the HITECH Act's tiered penalty structure based on culpability. Regarding the compliance history factor, HHS proposed that the Secretary must consider whether the current violation is the same or similar to "previous indications of noncompliance" rather than prior violations. (This change reflects the preference of HHS to reserve the term "violation" for use in "circumstances in which the Department has made a formal finding of a violation through a notice of proposed determination.")[433] HHS also proposed to apply the rule to business associates.[434]

Key Provisions of the Final Rule

Adopted as proposed.[435]

[429] 78 Fed. Reg. at 5584.
[430] 45 C.F.R. § 160.408.
[431] 78 Fed. Reg. at 5584.
[432] 75 Fed. Reg. at 40880-81.
[433] 78 Fed. Reg. at 5585.
[434] 78 Fed. Reg. at 5577.
[435] 78 Fed. Reg. at 5585.

Summary of Relevant Comments and HHS Response

One commenter requested that HHS limit the number of mitigating factors it will consider and exclude consideration of the entity's financial condition when determining the amount of a penalty. Some commenters were concerned that replacing "violations" with "indications of noncompliance" would create ambiguity and confusion. Others expressed support for the factors to be considered or requested additional examples and guidance regarding how the factors will be applied.[436]

With respect to the factors, HHS emphasized that the determinations will be a fact-specific inquiry and that it is important to consider all relevant factors. Regarding the use of the term "prior indications of noncompliance," HHS noted that a list of "violations" alone would not present an accurate picture of an entity's general history of compliance with the HIPAA Rules, which is relevant to determining the penalty. HHS clarified that a mere complaint does not constitute an indication of noncompliance, but prior investigations that yielded indications of noncompliance would constitute such a history, even if those indications were resolved by informal means.[437]

Analysis

The proposed changes are necessary to give effect to the HITECH Act's provisions. As in the section above, HHS declines to restrict its discretion with respect to enforcement, penalties, and the factors that will be relevant to those decisions.

45 C.F.R. § 160.410 – Affirmative Defenses

Relevant Statutory Provisions

Section 13410(d) of the HITECH Act removes an affirmative defense to the imposition of penalties if the covered entity did not know and with the exercise of reasonable diligence would not have known of the violation, and also prohibits the imposition of penalties for violations corrected within 30 days that were not the result of willful neglect.

Key Provisions of the Proposed Rule

The Interim Final Rule modified regulations to give effect to the HITECH Act's provisions. For violations occurring on or after February 18, 2009, covered entities may defend against civil money penalties by: (1) asserting that the violation is a wrongful disclosure of individually identifiable health information subject to criminal punishment under 42 U.S.C. § 1320d-6; or (2) establishing that the violation was not due to willful neglect and corrected either within 30 days of the date it obtained or should have

[436] 78 Fed. Reg. at 5584-85.
[437] 78 Fed. Reg. at 5585.

obtained knowledge of the violation or within the time period established by the Secretary.[438]

In the Proposed Rule, HHS proposed that, effective February 18, 2011, the Secretary may not impose civil money penalties for improper disclosures of individually identifiable health information if the covered entity or business associate has already received punishment under 42 U.S.C. § 1320d-6. In addition, the Proposed Rule made a conforming amendment to avoid retroactive application of a revised term.[439] HHS also proposed to apply the rule to business associates.[440]

Key Provisions of the Final Rule

Adopted as proposed.[441]

Summary of Relevant Comments and HHS Response

HHS did not receive any comments.[442]

Analysis

These modifications were necessary to give effect to statutory changes pursuant to the HITECH Act.

45 C.F.R. § 160.412 – Waiver

Relevant Statutory Provisions

Regulatory language in effect prior to February 18, 2009, implicitly recognized an affirmative defense that the covered entity did not know of the violation and, by exercising reasonable diligence, would not have known that the violation occurred. Section 13410(d) of the HITECH Act eliminates this affirmative defense, absent corrective action within 30 days, but does not revise the Secretary's waiver authority.[443]

Key Provisions of the Proposed Rule

The Interim Final Rule modified the regulations to provide that the Secretary may fully or partially waive the penalty "for violations due to reasonable cause and not willful neglect" if paying the penalty "would be excessive relative to the violation" and the covered entity has corrected the problem within the requisite time period.[444] In the

[438] 74 Fed. Reg. at 56128-29; 45 C.F.R. § 160.410.
[439] 78 Fed. Reg. at 5586.
[440] 78 Fed. Reg. at 5577.
[441] 78 Fed. Reg. at 5586.
[442] 78 Fed. Reg. at 5586.
[443] 78 Fed. Reg. at 5586.
[444] 74 Fed. Reg. at 56129; 45 C.F.R. § 160.412.

Proposed Rule, HHS proposed conforming amendments to align with the proposed revision to the affirmative defenses in Section 160.410.[445]

Key Provisions of the Final Rule

Adopted as proposed.[446]

Summary of Relevant Comments and HHS Response

A few commenters requested that the Secretary's waiver authority be extended to apply to penalties for violations of which a covered entity did not know or would not have known through the exercise of reasonable diligence, in addition to reasonable cause violations. HHS did not give a specific response, but referred commenters to the Proposed Rule, which addresses these concerns.[447]

Analysis

These conforming modifications were necessary to give effect to statutory changes pursuant to the HITECH Act.

45 C.F.R. § 160.418 – Penalty Not Exclusive

Relevant Statutory Provisions

None.

Key Provisions of the Proposed Rule

HHS proposed to incorporate a reference to a section of the Patient Safety and Quality Improvement Act (PSQIA) at 42 U.S.C. § 299b-22 providing that penalties are not to be imposed under both PSQIA and the HIPAA Privacy Rule for the same violation.[448]

Key Provisions of the Final Rule

Adopted as proposed.[449]

Summary of Relevant Comments and HHS Response

There were no substantive comments on this modification.[450]

[445] 78 Fed. Reg. at 5586.
[446] 78 Fed. Reg. at 5586.
[447] 78 Fed. Reg. at 5586.
[448] 78 Fed. Reg. at 5586.
[449] 78 Fed. Reg. at 5586.
[450] 78 Fed. Reg. at 5586.

Analysis

The Final Rule clarifies that duplicate penalties will not be imposed for a single violation of these two federal statutes.

45 C.F.R. § 160.420 – Notice of Proposed Determination

Relevant Statutory Provisions

None.

Key Provisions of the Proposed Rule

Section 160.420 requires the Secretary to mail to a covered entity or business associate written notice of its intent to impose a penalty. The notice must include information such as the statutory basis of the penalty and the facts giving rise to the penalty.[451] While not required by statute, the Interim Final Rule added the requirement that the Secretary identify in the notice of proposed determination the applicable violation category (tier) upon which the proposed penalty amount is based.[452]

Key Provisions of the Final Rule

Adopted as proposed.[453]

Summary of Relevant Comments and HHS Response

There were no substantive comments on this proposal.[454]

Analysis

This provision gives violators notice of the penalty tier being applied to the determination of their penalty.

[Calculation of the 30-day Cure Period for Willful Neglect Violations]

Relevant Statutory Provisions

HHS using its authority.

Key Provisions of the Proposed Rule

[451] 45 C.F.R. § 160.420.
[452] 74 Fed. Reg. 56129.
[453] 78 Fed. Reg. at 5586.
[454] 78 Fed. Reg. at 5586.

In the Interim Final Rule, HHS stated that it would look at when a covered entity first had actual or constructive knowledge of a violation due to willful neglect on a case-by-case basis.[455] Under the HITECH Act, the minimum penalty for a violation due to willful neglect that is corrected within 30 days is significantly less than that for a violation due to uncorrected willful neglect. The interaction of the 30-day correction period and the date of actual knowledge was unclear. Therefore, HHS sought comment on alternative approaches to calculating the beginning of the 30-day period for the purpose of determining the minimum penalty.[456]

Key Provisions of the Final Rule

The Final Rule retains the policy set forth in the Interim Final Rule that the 30-day cure period for violations due to willful neglect, like those not due to willful neglect, begins on the date that an entity first has actual or constructive knowledge of the violation.[457]

Summary of Relevant Comments and HHS Response

Some commenters were concerned that it would be difficult to determine when the cure period begins and that a business associate's knowledge of a violation could be imputed to the covered entity prior to the covered entity actually being notified of the violation. Others suggested that the 30-day period should begin when HHS notifies the covered entity of a complaint.[458]

HHS responded that the uncertainty inherent in a constructive knowledge standard provides an appropriate incentive that is consistent with the strengthened enforcement of the HIPAA Rules under the HITECH Act.[459]

Analysis

HHS retains the discretion to determine, on a case-by-case basis, the date actual or constructive knowledge of a violation began. This policy encourages self-correction and proactive establishment of a compliance program to prevent, detect, and correct indications of noncompliance.

General Administrative Requirements Applicable to All Rules

45 C.F.R. § 160.101 – Statutory Basis and Purpose

Relevant Statutory Provisions

[455] 74 Fed. Reg. 56128.
[456] 78 Fed. Reg. at 5586-87.
[457] 78 Fed. Reg. at 5587.
[458] 78 Fed. Reg. at 5587.
[459] 78 Fed. Reg. at 5587.

Sections 13400 – 13424 of the HITECH Act mandate a number of regulatory changes to the HIPAA Rules.[460]

Key Provisions of the Proposed Rule

Section 160.101 sets out the statutory basis and purpose of the HIPAA Rules.[461] The Proposed Rule modified Section 160.101 to include references to the provisions of the HITECH Act upon which most of the regulatory changes in the Proposed Rule are based.[462]

Key Provisions of the Final Rule

Adopted as proposed.[463]

Summary of Relevant Comments and HHS Response

None.

Analysis

None.

45 C.F.R. § 160.102 – Applicability

Relevant Statutory Provisions

The HITECH Act mandates that certain provisions of HIPAA apply to business associates.

Key Provisions of the Proposed Rule

Section 160.102 sets forth the entities that the HIPAA Rules apply to.[464] The Proposed Rule added a new paragraph to Section 160.102 to make clear that certain standards, requirements, and implementation specifications in Subchapter A apply to business associates, consistent with the requirements of the HITECH Act.[465]

Key Provisions of the Final Rule

Adopted as proposed.[466]

---

[460] HITECH Act, §§ 13400 – 13424.
[461] 45 C.F.R. § 160.101.
[462] 78 Fed. Reg. at 5570.
[463] 78 Fed. Reg. at 5570; 45 C.F.R. § 160.101..
[464] 45 C.F.R. § 160.102.
[465] 78 Fed. Reg. at 5570.
[466] 78 Fed. Reg. at 5570; 45 C.F.R. § 160.102(b)..

Summary of Relevant Comments and HHS Response

None.

Analysis

None.

45 C.F.R. § 160.103 – Definition of "Business Associate"/Inclusion of Patient Safety Organizations

Relevant Statutory Provisions

In order to implement the HITECH Act, the definition of "business associate" must be modified to conform the term to the statutory provisions of the Patient Safety and Quality Improvement Act of 2005 (PSQIA).[467] PSQIA provides that Patient Safety Organizations must be treated as business associates when applying the Privacy Rule.[468]

Key Provisions of the Proposed Rule

HHS proposed a number of modifications to the definition of "business associate."[469] Section 160.103 includes in the definition of "business associate" a list of the functions and activities a person may carry out on behalf of a covered entity that would create a business associate relationship between the person and the entity.[470] The Proposed Rule modified the definition of "business associate" by adding "patient safety activities" to the list of functions and activities a person may carry out on behalf of a covered entity that would create a business associate relationship between the person and the entity.[471]

Key Provisions of the Final Rule

Adopted as proposed.[472]

Summary of Relevant Comments and HHS Response

Comments were supportive of the proposed modification.[473]

Analysis

[467] HITECH Act § 13400-424; 42 U.S.C. § 299b-21, *et seq.*
[468] The Patient Safety and Quality Improvement Act of 2005 ("PSQIA"), Pub. L. No. 109-41 (July 29, 2005), *implemented by* The Patient Safety Rule, 42 CFR 3.10 (2008), *codified at* 42 U.S.C. 299b-21, et. seq., § 299b-22.
[469] 78 Fed. Reg. at 5570.
[470] 45 C.F.R. § 160.103, at ¶ (1)(i) of "Business Associate."
[471] 78 Fed. Reg. at 5570.
[472] 78 Fed. Reg. at 5570.
[473] 78 Fed. Reg. at 5570.

None.

45 C.F.R. § 160.103 – Inclusion of Health Information Organizations (HIO), E-Prescribing Gateways, and Other Persons That Facilitate Data Transmission; as Well as Vendors of Personal Health Records

Relevant Statutory Provisions

Section 13408 of the HITECH Act applies to organizations providing data transmission of protected health information to a covered entity (or its business associate) that require access to such information on a routine basis, and vendors that contract with a covered entity to allow that covered entity to offer a personal health record to patients as part of the covered entity's electronic health record. This section requires that such organizations and vendors be treated as business associates for purposes of HITECH and the HIPAA Privacy and Security Rules, and must enter into a written business associate contract or other arrangement with the covered entity in accordance with the HIPAA Rules. The section identifies Health Information Exchange Organizations, Regional Health Information Organizations and E-prescribing Gateways as examples of relevant data transmission organizations.[474]

Key Provisions of the Proposed Rule

The Proposed Rule modifies the definition of "business associate" to explicitly include the following entities: A Health Information Organization; E-Prescribing Gateway or other person that provides data transmission services with respect to protected health information to a covered entity and requires routine access to such information; and persons that offer a personal health record to individuals on behalf of a covered entity.[475]

Key Provisions of the Final Rule

The Final Rule adopts the modification to the definition of "business associate" as proposed.[476] The Rule modifies the definition of "business associate" to also includes a person or entity that creates, receives, **maintains**, or transmits protected health information on behalf of a covered entity for a function or activity regulated by HIPAA.[477] This additional modification is intended to clarify that entities that maintain or store protected health information on behalf of a covered entity are business associates, even if they do not actually view the protected health information they hold.[478]

Summary of Relevant Comments and HHS Response

[474] 78 Fed. Reg. at 5570; HITECH Act, § 13408.
[475] 78 Fed. Reg. at 5,570 – 571.
[476] 78 Fed. Reg. at 5571; 45 C.F.R. § 160.103, at ¶ (3) of "Business Associate."
[477] 78 Fed. Reg. at 5572 ; 45 C.F.R. § 160.103, at ¶ (1)(i) of "Business Associate").
[478] 78 Fed. Reg. at 5572, 574.

Commenters generally supported the inclusion of Health Information Organizations ("HIOs"), personal health record vendors, and similar entities in the definition of "business associate." Commenters requested a regulatory definition of HIOs, but HHS declined to provide one, in recognition of the expected evolution of the types of entities that may be considered an HIO. HHS anticipates issuing future website guidance on the types of entities that fall within the definition of business associate.[479]

Commenters sought additional clarification about what it means to have "access on a routine basis" to protected health information for purposes of determining when certain entities would be excluded from the definition of business associates as mere conduits for the transport of protected health information. Commenters also questioned when personal health record vendors would be providing a personal health record "on behalf of" a covered entity, and thus would be considered a business associate.[480] In response, HHS stated that determinations about each of these situations would be fact-specific, while providing relevant examples of the expanded definition. HHS intends to provide future guidance clarifying these distinctions.[481]

Analysis

Conduits handle protected health information on behalf of a covered entity, but they are not considered a business associate. The exception is a narrow one, and given the space devoted to its discussion, it is clearly a complex and important issue. The key distinction between a conduit and a business associate is access to protected health information, regardless of whether an entity actually makes use of its access to view the information it holds. The addition of the term "maintain" to the activities that would qualify an entity as a business associate broadens the reach of the HIPAA Rules, which data transmission organizations and personal health record vendors should be mindful of, as their role in maintaining protected health information impacts their degree of access to that information. A conduit provides mere courier services for a covered entity, while entities that maintain protected health information on behalf of a covered entity are business associates.[482] A conduit is in custody of protected health information for a transient period only to either transport that information from one location or another, or as otherwise required by law. Conversely, a business associate is in custody of protected health information for a more persistent period, such as for long-term storage. When an organization or vendor has prolonged access to protected health information due to its role in maintaining the record on behalf of the covered entity, a business associate designation is most likely applicable.

45 C.F.R. § 160.103 – Inclusion of Subcontractors

Relevant Statutory Provisions

[479] 78 Fed. Reg. at 5571.
[480] 78 Fed. Reg. at 5571.
[481] 78 Fed. Reg. at 5571 – 572.
[482] 78 Fed. Reg. at 5572.

None.

Key Provisions of the Proposed Rule

The Proposed Rule modifies the definition of "business associate" to provide that subcontractors of a covered entity[483] are business associates to the extent that they require access to protected health information. The Rule also added the term "subcontractor" to Section 160.103, defined as "a person who acts on behalf of a business associate, other than in the capacity of a member of the workforce of such business associate." The Proposed Rule noted that its definition of a subcontractor would apply to an agent or other person who acts on behalf of the business associate, even if the business associate has failed to enter into a business associate contract with the person.[484]

The Proposed Rules required "downstream entities" that work at the direction of or on behalf of a business associate and handle protected health information to comply with the applicable Privacy and Security Rule provisions in the same manner as the primary business associate. These downstream entities would incur liability for acts of noncompliance in the same manner as the primary business associate.[485]

Key Provisions of the Final Rule

The Final Rule adopts the proposed rule's modification of applying business associate provisions to subcontractors. The Final Rule modifies the definition of "business associate" in Section 160.103 to include "a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate."[486]

The Final Rule does not adopt the Proposed Rule's definition of "subcontractor" and instead defines subcontractor in Section 160.103 as "a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate."[487] Thus, this definition applies when a business associate is delegating a function, activity, or service that the business associate had agreed to perform for a covered entity or other business associate.[488] Additionally, the Final Rule requires that covered entities obtain satisfactory assurances required by the Rules from their business associates, and business associates must to do the same with regard to subcontractors, and so on, no matter how far "down the chain" the information flows.[489]

Summary of Relevant Comments and HHS Response

[483] 78 Fed. Reg. at 5572.
[484] 78 Fed. Reg. at 5572.
[485] 78 Fed. Reg. at 5573.
[486] 78 Fed. Reg. at 5573; 45 C.F.R. § 160.103, at ¶ (3)(iii) of "Business Associate."
[487] 78 Fed. Reg. at 5573; 45 C.F.R. § 160.103, at "Subcontractor."
[488] 78 Fed. Reg. at 5573.
[489] 78 Fed. Reg. at 5574.

The majority of commenters opposed extending the business associate provisions of the Rules to subcontractors. Commenters expressed concern that the expanded application of the business associate provisions could result in covered entities trying to establish direct business associate contracts with subcontractors.[490] HHS disagreed, noting that the Final Rule is clear that a covered entity is not required to enter into a contract or other arrangement with a business associate that is a subcontractor.[491] Commenters also questioned whether the expanded application may cause covered entities to prohibit business associates from establishing subcontractor relationships altogether.[492] HHS responded that making subcontractors directly liable for violations of the applicable provisions of the HIPAA Rules will actually help to alleviate covered entities' concern that protected health information is not adequately protected when provided to subcontractors.[493]

Several commenters asked for clarification regarding who would or would not be considered a subcontractor under the Proposed Rule's definition, and the change in definition in the Final Rule provides further clarity on this issue. HHS ensured that the business associate provision will be applied to entities that have an indirect relationship with a covered entity involving the creation, receipt, maintenance, or transmission of protected health information.[494] HHS offers examples of the practical application of the new definitions.[495]

Analysis

Sections 13401 and 13404 of HITECH create direct liability under the HIPAA Privacy and Security Rules for persons who are not covered entities but who create or receive protected health care information in order for a covered entity to perform its health care functions.[496] If a subcontractor performing a function for a business associate is able to avoid the liability imposed by HITECH simply because it does not have a direct relationship to the covered entity, this would result in an unacceptable lapse in the privacy and security protections for protected health information provided by HIPAA. By applying the definition of "business associate," and thus direct liability imposed by HITECH to subcontractors, ensures that individuals' protected health information remains sufficiently protected in the hands of persons who are not covered entities.[497]

It is worth noting that who is and is not excluded from the definition of a business associate as a conduit applies in the context of subcontractors as well. Contractors and

[490] 78 Fed. Reg. at 5573.
[491] 78 Fed. Reg. at 5573;45 C.F.R. §§ 164.308(b)(1), 164.502(e)(1)(i).
[492] 78 Fed. Reg. at 5573.
[493] 78 Fed. Reg. at 5573 - 574.
[494] 78 Fed. Reg. at 5573, 574.
[495] 78 Fed. Reg. at 5574.
[496] 78 Fed. Reg. at 5573; HITECH Act, §§ 13401, 13404 .
[497] 78 Fed. Reg. at 5574.

subcontractors are business associates to the extent that they create, receive, maintain, or transmit protected health information.[498]

45 C.F.R. § 160.103 – Exceptions to Business Associates

Relevant Statutory Provisions

None.

Key Provisions of the Proposed Rule

Sections 164.308(b)(2) and 164.502(e)(1)(ii) of the Privacy Rule describe circumstances in which a covered entity is not required to enter into a business associate contract or other arrangement with the recipient of the protected health information.[499] The Proposed Rule moved these descriptions to the definition of "business associate" in Section 160.103 as exceptions, making clear that recipients of protected health information in these circumstances will not be considered business associates.[500]

Key Provisions of the Final Rule

Adopted as proposed.[501]

Summary of Relevant Comments and HHS Response

None received.[502]

Analysis

This proposed change clarifies that a person or entity is a business associate if the person or entity meets the definition of "business associate," even if a covered entity (or business associate with respect to a subcontractor), fails to enter into a required business associate contract with the person or entity.

45 C.F.R. § 160.103 – Technical Changes to the Definition

Relevant Statutory Provisions

None.

Key Provisions of the Proposed Rule

[498] 78 Fed. Reg. at 5574.
[499] *See, e.g.*, 78 Fed. Reg. at 5574.
[500] 78 Fed. Reg. at 5574; 45 C.F.R. §§ 164.308(b)(2), 164.502(e)(1)(ii).
[501] 78 Fed. Reg. at 5574.
[502] 78 Fed. Reg. at 5574.

In Section 160.103, the definition of business associate utilized the term "individually identifiable information." The Proposed Rule changed this term "protected health information" in recognition of the fact that a business associate has no obligation under HIPAA with respect to individually identified health information unless it is also protected health information.[503]

Key Provisions of the Final Rule

Adopted as proposed.[504] The Final Rule also clarifies that its substantive modification of the definition of "business associate" to include an entity that "creates, receives, maintains, or transmits" protected health information on behalf of a covered entity is also technical in nature, designed to make the definition more consistent with the language in other sections of the Privacy and Security Rules.[505]

Summary of Relevant Comments and HHS Response

No substantial comments received.[506]

Analysis

None.

Summary of Relevant Comments Unrelated to a Particular Provision

The Final Rule responds to several questions regarding whether certain types of entities would be considered a business associate for purposes of the HIPAA Rules.[507]

- *Research***.** An external researcher is not a business associate by virtue of its research activities, even if the covered entity has hired the researcher to perform the research. A researcher may be a business associate if s/he performs a function, activity, or service for a covered entity that falls within the definition of business associate, such as creating a de-identified or limited data set for the covered entity.[508]
- *Finance/Banking***.** The Rules do not apply to banking and financial institutions with respect to the payment processing activities identified in Section 1179 of the HIPAA statute. A banking or financial institution may be a business associate where the institution performs functions above and beyond payment processing activities on behalf of a covered entity, such as performing accounts receivable functions on behalf of a health care provider.[509]

[503] 78 Fed. Reg. at 5574.
[504] 78 Fed. Reg. at 5574.
[505] 78 Fed. Reg. at 5574; 45 C.F.R. §§ 164.308(b) and 164.502(e).
[506] 78 Fed. Reg. at 5574.
[507] 78 Fed. Reg. at 5575.
[508] 78 Fed. Reg, at 5574-75.
[509] 78 Fed. Reg. at 5575.

- *Insurance***.** A business associate agreement is not required where a covered entity purchases a health plan product or other insurance from an insurer (specifically malpractice insurance). A business associate relationship could arise if the insurer is performing a function on behalf of, or providing services to, the covered entity that does not directly relate to the provision of insurance benefits and that involve access to protected health information.[510]

45 C.F.R. § 160.103 – Definition of Electronic Media

Relevant Statutory Provisions

None.

Key Provisions of the Proposed Rule

The Proposed Rule revised the definition of "electronic media" to reflect the development of new technology that could or have made existing terms and references in the definition obsolete.[511]

Key Provisions of the Final Rule

The Final Rule accepts the proposed modifications to the definition of "electronic media," with two additional modifications.[512] The Final Rule removes parenthetical language referring to "wide open" with respect to the Internet and "using Internet technology to link a business with information accessible only to collaborating parties" with respect to extranets and intranets. These parentheticals clarified certain key words that are now better understood, rendering such explanations unnecessary. The Final Rule also adds the word "immediately" to exclude transmissions when the information exchanged did not exist in electronic form immediately before transmission.[513]

Summary of Relevant Comments and HHS Response

Commenters were supportive of the revised definition and the flexibility created to account for technological developments.[514] HHS clarified in response to several commenters that protected health information stored, intentionally or not, in office machines is subject to the Privacy and Security Rules, except where the "immediately" exclusion applies.[515]

Analysis

[510] 78 Fed. Reg. at 5575.
[511] 78 Fed. Reg. at 5575; 45 C.F.R. § 160.103.
[512] 78 Fed. Reg. at 5576; 45 C.F.R. § 160.103, at the definition of "electronic media."
[513] 78 Fed. Reg. at 5576.
[514] 78 Fed. Reg. at 5575.
[515] 78 Fed. Reg. at 5576.

Although office machines are not generally relied upon for storage and access to stored information, covered entities and business associates should be aware that these devices are capable of storing protected health information, and must ensure any protected health information stored on such devices is appropriately protected and secured from inappropriate access. Further, before removal of the device from the covered entity or business associate, proper safeguards should be followed to remove the electronic protected health information from the machine.

45 C.F.R. § 160.103 – Definitions of Protected Health Information

Relevant Statutory Provisions

None.

Key Provisions of the Proposed Rule

The Proposed Rule modified the definition of "protected health information" to provide that the Privacy and Security Rules did not protect the individually identifiable health information of a person who has been deceased for more than 50 years.[516]

Key Provisions of the Final Rule

Adopted as proposed.[517]

Summary of Relevant Comments and HHS Response

None.

Analysis

None.

45 C.F.R. § 160.103 – Definition of State and other Relevant Changes

Relevant Statutory Provisions

None.

Key Provisions of the Proposed Rule

In order to ensure consistency across definitions, and to bring various definitions into conformance with other HIPAA provisions and with certain sections of the HITECH Act, the Proposed Rule made the following technical modifications to Section 160.103:[518]

[516] 78 Fed. Reg. at 5576; 45 C.F.R. §§ 160.103, 164.502(f).
[517] 78 Fed. Reg. at 5576.
[518] 78 Fed. Reg. at 5576; 45 C.F.R. § 160.103.

- Relocate the definitions of "administrative simplification provision," "ALJ" "civil monetary penalty," "respondent," and "violation or violate" from § 160.302 to § 160.103 for ease of reference;
- Add a reference to HITECH §§ 13400 – 13424 to the definition of "administrative simplification provision" at § 160.103;
- Replace the term "individually identifiable health information" with "protected health information" in the definition of "standard" at § 160.103;
- Add a reference to "business associate" following the reference to "covered entity" in the definitions of "respondent" and "compliance date," at §160.103;
- Revise the definition of "workforce member" in § 160.103 to reflect the obligations that some provisions of the HITECH Act and the Privacy and Security Rules place on business associates with respect to workforce members; and
- Add reference to American Samoa and the Commonwealth of the Northern Mariana Islands in the definition of "State" at § 160.103, consistent with HITECH § 13400.

Key Provisions of the Final Rule

Adopted as proposed.[519]

Summary of Relevant Comments and HHS Response

None.

Analysis

None.

45 C.F.R. § 160.201 – Statutory Basis

Relevant Statutory Provisions

HHS using its regulatory authority.

Key Provisions of the Proposed Rule

In the prior rule, Section 160.201 was titled "Applicability" and stated that the provisions of Subpart B "implement Section 1178 of the Act, as added by Section 262 of Public Law 104-191."[520] HHS proposed to change the title to "Statutory Basis" and insert references to HIPAA Section 264(c), which references the statutory basis for the exception from preemption for laws that are more stringent than the HIPAA Privacy Rule, and the

[519] 78 Fed. Reg. at 5576.
[520] 45 C.F.R. § 160.201.

HITECH Act Section 13421(a), which applies HIPAA's preemption rules to the privacy and security provisions of the HITECH Act.[521]

Key Provisions of the Final Rule

Adopted as proposed.[522]

Summary of Relevant Comments and HHS Response

Commenters were concerned about the lack of uniform federal and state privacy laws and the confusion and expense that results with operating across state lines in such an environment. HHS noted that it is a statutory requirement for the HIPAA Privacy Rule to provide a federal floor of privacy protection with the possibility of more stringent state laws.[523]

Analysis

This modification is consistent with the HIPAA and HITECH statutes and serves to clarify the statutory basis for the provisions regarding preemption of state law.

45 C.F.R. § 160.202 – Definitions

Relevant Statutory Provisions

HHS using its regulatory authority.

Key Provisions of the Proposed Rule

The term "contrary," when used to compare a state law and federal regulation, means that compliance with both the law and regulation is impossible for covered entities or that the state law impedes the full execution of HIPAA.[524] HHS proposed to insert references to business associates in Paragraph 1 and to all of the sections of Subtitle D of the HITECH Act in Paragraph 2 of the definition.[525]

The term "more stringent" refers to state laws falling within one of six specified categories that have standards, requirements, or specifications greater or more onerous than those required by the Privacy Rule. The first category includes laws that "prohibit[] or restrict[] a use or disclosure in circumstances" that would otherwise be permitted under the subchapter, except disclosures that HHS requires in order to determine a covered entity's compliance or disclosures to individuals of their own individually

[521] 78 Fed. Reg. at 5576-77.
[522] 78 Fed. Reg. at 5577.
[523] 78 Fed. Reg. at 5577.
[524] 45 C.F.R. § 160.202.
[525] 78 Fed. Reg. at 5577.

identifiable health information.[526] HHS proposed to insert a reference to business associates.[527]

Key Provisions of the Final Rule

Adopted as proposed.[528]

Summary of Relevant Comments and HHS Response

HHS did not receive substantive public comment.[529]

Analysis

These modifications are not substantial, but serve to bring the regulations in line with the HITECH breach notification rule.[530]

Overview

The Final Rule incorporates changes that were made in the October 2009 Interim Final Rule,[531] which updated the HIPAA Enforcement Rule to reflect statutory amendments made by the HITECH Act and applied immediately to violations occurring after the HITECH Act's enactment on February 18, 2009. The Final Rule also incorporates changes in the Proposed Rule which reflected other provisions of the HITECH Act, including some that became effective on February 18, 2010, or a later date. In addition to the modifications described below, the Final Rule adds the term "business associate" to the following provision of the Enforcement Rule in order to implement HITECH Act Sections 13401 and 13404: Sections 160.300; 160.304; 160.306(a) and (c); 160.308; 160.310; 160.312; 160.316; 160.401; 160.402; 160.404(b); 160.406; 160.408(c) and (d); and 160.410(a) and (c).[532]

45 C.F.R. § 164.102- Statutory Basis

Relevant Statutory Provisions

Statutory and regulatory changes are based on Sections 13400-13424 of the HITECH Act. [533]

Key Provisions of the Proposed Rule

[526] 45 C.F.R. § 160.202.
[527] 78 Fed. Reg. at 5577.
[528] 78 Fed. Reg. at 5577.
[529] 78 Fed. Reg. at 5577.
[530] HITECH Act § 13402.
[531] 74 Fed. Reg. at 56123.
[532] 78 Fed. Reg. at 5577.
[533] HITECH Act § 13400-13424.

HHS proposed a technical change to include a reference to the provisions of the HITECH Act noted above, which is the basis for the regulatory changes discussed. [534]

Key Provisions of the Final Rule

Adopted as proposed. [535]

Summary of Relevant Comments and HHS Response

There were no substantive comments on this section.

Analysis

None.

General Administrative Requirements Applicable to Privacy, Security and Breach Notification Rules

45 C.F.R. § 164.104 -Applicability

Relevant Statutory Provisions

The HITECH Act requires that this provision of Part 164 also applies to business associates. [536]

Key Provisions of the Proposed Rule

The Proposed Rule replaced Section 164.104(b) so that the standards, requirements, and implementation specifications of the HIPAA Privacy, Security and Breach Notification Rules apply to business associates. The Proposed Rule also removed language in (b) requiring health care clearinghouses to comply with Section 164.105 regarding the organizational requirements of a covered entity. [537]

Key Provisions of the Final Rule

Adopted as proposed. [538]

Summary of Relevant Comments and HHS Response

[534] 78 Fed. Reg. at 5587.
[535] 78 Fed. Reg. at 5587.
[536] HITECH Act § 13401(a).
[537] 78 Fed. Reg. at 5587-88.
[538] 78 Fed. Reg. at 5587-88.

There were no substantive comments on this section.

Analysis

None.

45 C.F.R. § 164.105(a)(2)(ii)(C)-(E) – Organizational Requirements

Relevant Statutory Provisions

Under HITECH, Section 164.105 applies to Subpart D of Part 164, regarding breach notification of unsecured protected health information, which renders the specific references to the Privacy and Security Rules unnecessary. [539]

Key Provisions of the Proposed Rule

The Proposed Rule removed the paragraph requiring a covered entity to ensure that any component that performs business associate-like activities complies with the Privacy and Security Rules, as this was already established in the Rule. [540] The Proposed Rule also requested comments on whether a covered entity that is a hybrid entity should be required to include a component that performs business associate-like activities within the health care component.[541]

Key Provisions of the Final Rule

Adopted as proposed because the Final Rule has established that business associates can be directly liable for a violation of the Security and Privacy Rules. [542] The Final Rule includes business associate functions within the health care component of the hybrid entity in order to prevent a hybrid entity from avoiding direct liability.[543]

Summary of Relevant Comments and HHS Response

Many commenters recommended that hybrid entities retain the flexibility to include business associates in the health care component, which would allow the covered entity to distinguish the functions of the business associates from the health care component. Others argued that the requirement to include business associates would be burdensome. There was some support for the requirement. HHS agreed with those in support of requiring hybrid entities to include business associate functions within the health care

[539] HITECH Act § 13402.
[540] 78 Fed. Reg. at 5588; 45 C.F.R. §164.105(a)(2)(ii)(C)-(E).
[541] 78 Fed. Reg. at 5588.
[542] 78 Fed. Reg. at 5588.
[543] 78 Fed. Reg. at 5588.

component.[544]

Analysis

None.

45 C.F.R. § 164.105(a)(2)(iii)(C) – Organizational Requirements

Relevant Statutory Provisions

None.

Key Provisions of the Proposed Rule

The Proposed Rule added a new paragraph that makes the covered entity itself responsible for complying with Sections 164.314 and 164.504 regarding business associate arrangements and other organizational requirements with respect to hybrid entities.[545]

Key Provisions of the Final Rule

Adopted as proposed.[546]

Summary of Relevant Comments and HHS Response

There were no substantive comments on this section.

Analysis

None.

Preemption

Relevant Statutory Provisions

Section 1128 of the Social Security Act provides that HIPAA administrative simplification provisions generally preempt conflicting state law.[547]

Section 13421 of HITECH applies Section 1128 of the Social Security Act to its provisions and requirements.[548]

[544] 78 Fed. Reg. at 5588.
[545] 78 Fed. Reg. at 5589.
[546] 78 Fed. Reg. at 5589.
[547] Social Security Act, § 1178, 42 U.S.C. § 1320d-7.
[548] HITECH Act, § 13421(a).

Key Provisions of the Proposed Rule

The Interim Final Rule clarified that contrary state law will be preempted by these breach notification regulations.[549]

Key Provisions of the Final Rule

The Final Rule maintains the preemption standard discussed in the Interim Final Rule.[550]

Summary of Relevant Comments and HHS Response

Several commenters expressed confusion and concern with the preemption standard, noting that there will be some cases in which a covered entity will have to provide multiple notices to the same individual to ensure compliance with all relevant laws, which could result in confusion for the individual and increased costs for the covered entity. HHS believes that covered entities will generally be able to comply with both state and federal requirements for providing breach notification with one breach notice, but in the event that there is an exceptional case, HHS lacks the authority to preempt state laws that are not contrary to the Rule.[551]

Analysis

None.

[549] 78 Fed. Reg. at 5658.
[550] 78 Fed. Reg. at 5658.
[551] 78 Fed. Reg. at 5658.