Highlights of the Final Omnibus HIPAA Rule

Health Information & the Law Project[1]
Jane Hyatt Thorpe, JD
Lara Cartwright-Smith, JD, MPH
Devi Mehta, JD, MPH
Elizabeth Gray, JD
Teresa Cascio, JD
Grace Im, JD

January 30, 2013

Background

On January 17, 2013, the U.S. Department of Health and Human Services (HHS) released the long-awaited omnibus Final Rule[2] including modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules required by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)[3] and revisions to the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act of 2008 (GINA).[4] HHS also used its regulatory authority to make additional changes to make the rules consistent with other Departmental regulations.

Since the passage of HIPAA in 1996[5] and promulgation of the HIPAA Privacy, Security, and Enforcement Rules,[6] there has been significant legislative activity affecting how health

[1] Health Information & the Law (www.HealthInfoLaw.org) is a project of the George Washington University School of Public Health and Health Services' Hirsh Health Law and Policy Program developed with support from the Robert Wood Johnson Foundation. The project 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 website 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] 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).
[3] 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).
[4] 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.).
[5] 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.).
[6] Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462 (December 28, 2000).

information may be used and disclosed, including changes to the privacy and security requirements as well as expanded and new requirements for the enforcement process (including penalties) and breach notification. Specifically, the HITECH Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA),[7] is designed 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. It also included new notification requirements for breaches of unsecured protected health information. Also since the promulgation of the original HIPAA rules, GINA was enacted to prohibit the use of genetic information by certain health plans for underwriting purposes and required changes to the HIPAA Privacy Rule to specifically protect genetic information like other protected health information.

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 were included in a proposed rule on July 14, 2010.[8]
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.[9]
3) Final rule implementing changes to the Breach Notification for Unsecured Protected Health Information Rule as required by HITECH that was published as an Interim Final Rule on August 24, 2009.[10]
4) Final rule modifying the HIPAA Privacy Rule as required by GINA that was published as a proposed rule on October 7, 2009.[11]

This Final Rule does not address the HITECH accounting for disclosures requirement[12] that was addressed in a proposed rule on May 31, 2011.[13] HHS indicated that a separate final rulemaking will be released in the future.

[7] American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009).
[8] 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).
[9] HIPAA Administrative Simplification: Enforcement; Interim Final Rule with Request for Comments, 74 Fed. Reg. 56123 (October 30, 2009).
[10] Breach Notification for Unsecured Protected Health Information; Interim Final Rule with Request for Comments, 74 Fed. Reg. 42740 (August 24, 2009).
[11] 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).
[12] HITECH Act, § 13405.
[13] 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 (May 31, 2011) (to be codified at 45 C.F.R. Part 164).

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 overview highlights key changes of the four prior rulemakings in this Final Rule. A longer, more comprehensive analysis will be released shortly.

I. HIPAA Privacy, Security, and Enforcement Rules

The HIPAA Privacy Rule[14] requires certain covered entities (providers, health plans and clearinghouses) to ensure the privacy of protected health information and sets forth the circumstances under which a covered entity is required or may use or disclose protected health information. The Privacy Rule also provides individuals rights to their protected health information such as the right to examine, request corrections, and request a copy. The Rule also allows covered entities to enter into contractual arrangements with business associates to do work on their behalf so long as the business associate protects the protected health information and only uses and discloses the protected health information according to the terms of its agreement with the covered entity.

The HIPAA Security Rule[15] requires covered entities to establish and maintain certain administrative, physical, and technical safeguards to protect electronic protected health information. If a covered entity contracts with a business associate to do work on their behalf, the contract or arrangement must provide satisfactory assurances that the business associate will similarly meet the Security Rule requirements for any electronic protected health information they create, receive, maintain, or transmit on behalf of the covered entity.

The HIPAA Enforcement Rule[16] governs the enforcement process, including HHS investigations, requirements for setting the amount of a civil monetary penalty if a violation occurs, and requirements for hearings and appeals if a covered entity challenges a violation.

Business Associates

The most significant changes required by HITECH and implemented by the Final Rule relate to business associates.

[14] The HIPAA Privacy Rule, 45 CFR Part 160 and Subparts A and E of Part 164.
[15] The HIPAA Security Rule, 45 CFR Part 160 and Subparts A and C of Part 164.
[16] The HIPAA Enforcement Rule, 45 CFR Part 160, Subparts C – E.

Direct Liability: Prior to HITECH, the HIPAA Privacy, Security, and Enforcement Rules did not directly govern or penalize business associates for noncompliance; rather the business associate contracts between a covered entity and a business associate governed enforcement and penalties. As required by HITECH and finalized in this Final Rule, specific requirements of the Privacy Rule now directly apply to business associates and make them directly liable for noncompliance with those requirements as well as those included in their business associate agreement.[17] Similarly, the administrative, physical, and technical safeguard requirements in the Security Rule as well as the policies, procedures, and documentation requirements also directly apply to business associates in the same manner as they apply to covered entities.[18] Finally, the enforcement process, including civil and criminal penalties for violations of the Privacy and Security Rules, now directly applies to business associates in the same manner as it applies to covered entities.[19]

As noted above, business associates are not required to meet all requirements of the Privacy Rule.[20] While the substantive provisions that relate to the use and disclosure of protected health information (such as the requirements for disclosure to an individual and for compliance with the minimum necessary standard) now apply to business associates, they are not required to provide a notice of privacy practices or designate a privacy official unless a covered entity has obligated the business associate to do so on its behalf.[21] In these latter cases, liability for the business associate would be based on the contractual requirements.[22]

Expanded Definition of Business Associate: The definition of "business associate" now includes "(1) 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 that requires routine access to such protected health information; and (2) a person who offers a personal health record to one or more individuals on behalf of a covered entity."[23] HHS declined to define "Health Information Organization," but indicated that it includes an organization that oversees and governs the exchange of health-related information among organizations.[24] However, HHS did indicate intent to provide future guidance on when a personal health record vendor would be considered a business associate as well as guidance on entities that provide data transmission services are business associates and when a conduit exception to the definition of business associate would apply with respect to electronic health information exchange activities.[25] HHS also added "patient safety activities" to the list of activities a business

[17] HITECH Act §13404(a); 45 C.F.R. § 164.104(b); 78 Fed. Reg. at 5591.
[18] HITECH Act, § 13401; 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.316; 78 Fed Reg. at 5589.
[19] HITECH Act, §13404; 45 C.F.R. § 164.502(a).
[20] HITECH Act, §13404; 45 C.F.R. § 164.500.
[21] 78 Fed. Reg. at 5591.
[22] HITECH Act, §13404; 45 C.F.R. § 164.500.
[23] 45 C.F.R § 160.103, 78 Fed. Reg. at 5688.
[24] 78 Fed. Reg. at 5571.
[25] 78 Fed. Reg. at 5571.

associate may conduct on behalf of a covered entity that would create a business associate arrangement, in conformance with the Patient Safety Quality Improvement Act.[26]

In addition, the Final Rule establishes that a business associate does not become a business associate just by virtue of contracting with a covered entity, but rather by meeting the definition of a business associate (i.e., "when a person creates, receives, maintains, or transmits protected health information on behalf of a covered entity or business associate and otherwise meets the definition of a business associate").[27] Furthermore, liability does not depend on the type of protected health information or the type of entity involved.[28]

HHS also used its regulatory authority to expand the definition of "business associate" to include subcontractors of a business associate (i.e., those persons a business associate engages to perform the business associate's obligation to the covered entity that requires access to protected health information).[29] Covered entities are not required to enter into business associate agreements with subcontractors; rather that obligation lies with the business associate of the covered entity.[30]

Finally, HHS clarified that the definition of business associate does not include health care providers that receive protected health information for treatment purposes, plan sponsors that receive protected health information from group health plans under certain circumstances, or government agencies that receive or collect protected health information to determine eligibility for a government health plan providing public benefits.[31]

Business Associate Agreement: HHS clarified that even given the new direct liability for business associates, the HITECH Act expressly ties liability to compliance with business associate agreements.[32] In addition, there may be circumstances where the business associate is contractually required to perform certain activities for which direct liability does not apply and thus the business associate agreement would control (*i.e.*, amending protected health information).[33] HHS also expanded the required elements of a business associate agreement to include provisions requiring business associates to comply with the Security Rule where applicable, report breaches of unsecured protected health information to covered entities, and ensure that subcontractors that create or receive protected health information on behalf of a business associate meet the same restrictions and conditions that apply to the business associate.[34] Finally, HITECH specifically requires certain vendors (data transmission and

[26] Patient Safety and Quality Improvement Act of 2005 (PSQIA), Public Law 109-41, 42 U.S.C. 299b-21 et seq., §922(i); 45 C.F.R.§ 164.501; 78 Fed. Reg. at 5592.
[27] 45 C.F.R. § 164.502(a); 78 Fed. Reg. at 5598.
[28] 78 Fed. Reg. at 5598.
[29] 45 C.F.R. § 164.308(b); 78 Fed. Reg. at 5590.
[30] 45 C.F.R. § 164.308(b); 78 Fed. Reg. at 5590.
[31] 45 C.F.R. § 160.103; 78 Fed. Reg. at 5574.
[32] HITECH Act, § 13404; 45 C.F.R. § 164.502(e); 78 Fed. Reg. at 5590.
[33] 78 Fed. Reg. at 5681.
[34] 45 C.F.R. § 164.504(e); 78 Fed. Reg. at 5600.

personal health record) to have business associate agreements with the covered entities to which they provide services.[35]

Transition Period: HHS finalized its proposal to allow covered entities and business associates to continue to operate under existing contracts for up to one year past the compliance date of Final Rule (September 23, 2013), provided the contracts met the requirements of the prior HIPAA Rules and were not renewed or modified between the effective and compliance date of the Final Rules.[36] Despite requests from commenters to extend this period longer than one year, HHS declined to do so.[37]

Limitations on Use and Disclosure of Protected Health Information for Marketing and Fundraising Purposes

Marketing: The current Privacy Rule requires covered entities to obtain authorization from an individual prior to using or disclosing protected health information for marketing purposes except for face-to-face communications or to provide a nominal promotional gift. In the Final Rule, HHS maintained the general definition of marketing meaning "to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service" and the existing exceptions.[38] In addition, HHS finalized two of three additional proposed exceptions for treatment and health care operations communications about health-related products or services.[39] 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.[40] 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.[41] These two exceptions to the definition of "marketing" were finalized. HHS did not 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.[42] In sum, HHS is requiring authorizations for all communications related to treatment and health care operations if the covered entity receives financial remuneration for the communication from a third party whose

[35] HITECH Act § 13408.
[36] 45 C.F.R. § 164.532(d) and (e); 78 Fed. Reg. at 5603.
[37] 78 Fed. Reg. at 5603.
[38] HITECH Act §13406(a); 45 C.F.R. § 164.501(b); 78 Fed. Reg. at 5595.
[39] 45 C.F.R. § 164.501; 78 Fed. Reg. at 5595.
[40] 45 C.F.R. § 164.501; 78 Fed. Reg. at 5592.
[41] 45 C.F.R. § 164.501; 78 Fed. Reg. at 5596.
[42] 78 Fed. Reg. at 5596.

product or service is being marketed.[43]

HHS defines "financial remuneration" as "direct or indirect payment from or on behalf of a third party whose product is being described."[44] This does not include payment for treatment of an individual or in-kind services. The key question is whether there is payment for the communication.[45]

Fundraising: HHS generally finalized the provisions of the proposed rule related to fundraising. First, with every fundraising communication, a covered entity must provide an opportunity to opt out of receiving future fundraising communications.[46] Although HHS solicited comments on multiple methods of communication to allow individuals to opt out from receiving fundraising communications, HHS will allow covered entities to determine which method or methods work best provided the selected method does not impose an undue burden or more than nominal cost on individuals.[47] HHS provided several examples of acceptable methods including the use of a toll-free number or email address. Second, a covered entity may not condition treatment or payment on an individual's decision to receive or not receive fundraising communications.[48] Third, a covered entity may not send fundraising communications to individuals that have opted out (as opposed to the current requirement to use "reasonable efforts").[49]

In addition, covered entities must include in their notice of privacy practices that individuals may be contacted to raise funds for the covered entity and may opt out of such communications.[50] However, the Final Rule does not require covered entities to send pre-solicitation opt-out notices to individuals in advance of a fundraising communication.[51]

HHS also expanded the categories of information covered entities may use to target fundraising communications to individuals. To the previously approved categories of demographic information, health insurance status, and dates of health care provided to the individual, the Final Rule also allows covered entities to use and disclose department of service information, treating physician information, and outcome information for fundraising purposes.[52]

Prohibition on Sale of Protected Health Information Without Individual Authorization

As required by HITECH, the Final Rule adds a third circumstance under which a covered entity

[43] 78 Fed. Reg. at 5596-97.
[44] 78 Fed. Reg. at 5595.
[45] 78 Fed. Reg. at 5595-96.
[46] 45 C.F.R. § 164.514(f)(2)(ii).
[47] 45 C.F.R. § 164.514(f)(2)(ii); 78 Fed. Reg. at 5619.
[48] 45 CFR § 164.524(c)(2)(ii).
[49] 45 CFR § 164.514(f); 78 Fed. Reg. at 5621.
[50] 45 C.F.R. §§ 164.514(f)(2)(i); 164.520(b)(1)(iii)(A); 78 Fed. Reg. at 5624.
[51] 78 Fed. Reg. at 5622.
[52] 45 C.F.R. § 164.514(f)(2)(ii); 78 Fed. Reg. at 5622.

must obtain a valid written authorization from the person who is the subject of the protected health information. In addition to most uses and disclosures of psychotherapy notes and marketing purposes,[53] covered entities will now be required to obtain authorization if the covered entity receives direct or indirect remuneration for the protected health information.[54] HHS also finalized several HITECH exceptions to this general prohibition on the sale of protected health information including: 1) public health activities;[55] 2) research purposes[56] if the price charged reflects the cost of preparation and transmittal of the information for research purposes; 3) treatment and payment purposes;[57] 4) the sale, transfer, merger or consolidation of all or part of a covered entity or an entity that following such activity will become a covered entity and for related due diligence;[58] 5) services rendered by a business associate pursuant to a business associate agreement and at the request of the covered entity;[59] 6) providing an individual with access to his or her protected health information or an accounting of disclosures pursuant to the law;[60] 7) disclosures required by law;[61] and 8) other purposes as HHS deems necessary and appropriate by regulation. This prohibition becomes effective six months after the effective date of the Final Rule. (The Final Rule is effective on March 26, 2013, so covered entities and business associates must comply as of September 23, 2013.)[62]

Defined Sale of Protected Health Information: In response to numerous commenter requests, HHS included a definition of "sale of protected health information" to generally mean "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."[63]

Existing authorizations*:* HHS clarified that permissions existing prior to the compliance date of the Final Rule even if the authorization does not indicate that the disclosure is made in return for remuneration, will be honored for up to one year from the effective date of the Final Rule so long as the permission is not modified or extended during that time.[64]

Limited Data Set: HHS declined to exempt a limited data set from the prohibition on the sale of protected health information because it still constitutes protected health information.[65] HHS did

[53] HITECH Act, §13405(d); 45 C.F.R. § 164.508.
[54] HITECH Act, §13405(d); 45 C.F.R. § 164.508; 78 Fed. Reg at 5606.
[55] 45 C.F.R. §§ 164.502(a)(5)(ii)(B)(2)(i); 164.512(b); 164.514(e).
[56] 45 C.F.R. §§ 164.502(a)(5)(ii)(B)(2)(ii); 164.501; 164.512(i).
[57] 45 C.F.R. §§ 164.502(a)(5)(ii)(B)(2)(iii); 164.512(i); 164.514(e).
[58] 45 C.F.R. §§ 164.502(a)(5)(ii)(B)(2)(iv); 164.506(a).
[59] 45 C.F.R. §§ 164.502(a)(5)(ii)(B)(2)(v); 164.502(e); 164.504(e).
[60] 45 C.F.R. §§ 164.502(a)(5)(ii)(B)(2)(vi); 164.524; 164.528.
[61] 45 C.F.R. §§ 164.502(a)(5)(ii)(B)(2)(vii); 164.512(a).
[62] HITECH Act, § 13405(d)(4); 78 Fed. Reg. at 5606.
[63] HITECH Act, § 13405(d)(1); 45 C.F.R. § 164.502(a)(5)(ii)(B)(1); 78 Fed. Reg. at 5606.
[64] 45 C.F.R. § 164.532(f); 78 Fed. Reg. at 5609.
[65] 78 Fed. Reg. at 5609.

clarify that disclosures of limited data sets for permitted purposes would be exempt from the authorization requirements to the extent the remuneration is a reasonable, cost-based fee for preparation and transmission of the data. HHS also clarified that a covered entity may continue to use or disclose a limited data set in accordance with an existing data use agreement for one year from the compliance date of the Final Rule so long as the agreement is not renewed or modified sooner.[66]

Expansion of Individuals Rights to Restrict Use and Disclosure and Access Health Information

Right to Restrict Disclosures: As addressed by HITECH, the Final Rule requires a covered entity to comply with an individual's request to restrict the use or disclosure of his or her protected health information for payment, treatment or health care operations purposes if the restriction applies to protected health information pertaining to a health care service that the provider has been paid out of pocket in full for, unless disclosure is authorized by law.[67] Under the current Privacy Rule, covered entities were not required to agree to requested restrictions. HHS did clarify that covered health care providers are not required to create separate medical records or otherwise segregate patient restricted protected health information. However, they will need a system to identify protected health information that has been restricted by the individual to ensure that the information is not inadvertently disclosed to a health plan for payment or health care operations purposes. A provider who does disclose restricted protected health information to a health plan will be in violation of the Privacy Rule and the HITECH Act and subject to criminal penalties, civil monetary penalties, or corrective actions.[68]

Right to Access: If an individual requests access to his or her protected health information, and such information is maintained in an electronic designated record set, a covered entity must provide the individual with a copy of the information in the electronic form or format that the individual requests, if that form or format is readily producible.[69] If the information is not readily producible, then the covered entity must provide the information in a readily readable electronic format as agreed to by the covered entity and the individual.[70] HHS defines "machine readable" to mean digital information stored in a standard format enabling the information to be processed and analyzed by computer (e.g., MS Word or Excel, text, HTML, or text- based PDF, etc.).[71] This requirement applies to all electronic protected health information regardless of whether the information is maintained in an electronic health record or other electronic format.

Third Parties: The Final Rule also requires a covered entity to transmit a copy of protected

[66] 78 Fed. Reg. at 5609.
[67] HITECH Act §13405(a); 45 C.F.R. § 164.522; 78 Fed. Reg. at 5628.
[68] 78 Fed. Reg. at 5628-29.
[69] 45 C.F.R. § 164.524(c)(2)(ii); 78 Fed. Reg. at 5631.
[70] 45 C.F.R. § 164.524(c)(2)(i).
[71] 78 Fed. Reg. at 5631.

health information to another person designated by the individual if requested.[72] The request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the protected health information. This written request is distinct from an authorization form that includes additional required statements and elements.[73]

Fees: Covered entities may charge reasonable, cost-based fees for providing electronic copies of protected health information to an individual or their designee.[74] To determine cost, a covered entity may include the labor for copying protected health information as well as the cost of supplies for creating a paper copy or electronic media (e.g. CD or flash drive),[75] including postage charges.[76] Fees associated with maintaining systems for data access and storage are not considered reasonable, cost-based fees and may not be included.[77]

Timeliness: HHS finalized the proposal to allow covered entities 30 days to respond to an individual's request for his or her protected health information, but removed the timeliness provision allowing a covered entity 60 days to provide an individual with access to protected health information that is not maintained or accessible on-site.[78] HHS retained the opportunity for a covered entity to request a one-time extension of 30 days to respond to an individual's request.[79]

Modifications and Redistribution of Notice of Privacy Practices

HHS makes a number of significant changes to the Notice of Privacy Practices requirements in the current Privacy Rule to ensure that individuals are aware of the changes made by HITECH, GINA, and HHS in this Final Rule. While HHS makes clear that a Notice of Privacy Practices must not include a list of all circumstances in which authorization is required prior to disclosure, a Notice of Privacy Practices must include the following statements:

1) "[M]ost uses and disclosures of psychotherapy notes (where appropriate), uses and disclosures of protected health information for marketing purposes, and disclosures that constitute a sale of protected health information require authorization."[80]
2) Any other uses and disclosures not described in the Notice of Privacy Practices will only be made with prior authorization.[81]
3) An individual may opt out of receiving fundraising communications if the

[72] 45 C.F.R. § 164.524(c)(3); 78 Fed. Reg. at 5634.
[73] 45 C.F.R. § 164.508(c)).
[74] 78 Fed. Reg. at 5635-36.
[75] 45 C.F.R. §§ 164.524(c)(4)(i); 164.524(c)(4)(ii).
[76] 45 C.F.R. § 164.524(c)(4)(iii).
[77] 78 Fed. Reg. at 5636.
[78] 45 C.F.R. § 164.524(b).
[79] 45 C.F.R. § 164.524(b)(2)(ii); 78 Fed. Reg. at 5637.
[80] 45 C.F.R. § 164.520(b)(1)(ii)(E); 78 Fed. Reg. at 5623-24.
[81] 45 C.F.R. § 164.520(b)(1)(ii)(E); 78 Fed. Reg. at 5623-24.

organization intends to make such communications.[82]

4) An individual may restrict certain disclosures of protected health information if they pay out of pocket.[83]
5) Affected individuals have the right to be notified of a breach.[84]
6) Disclosure of protected health information that is genetic information for underwriting purposes is prohibited.[85]

Most importantly, HHS clearly indicates that these changes to the Notice of Privacy Practices represent "material" changes and thus covered entities must revise and redistribute Notices.[86]

Modification to Individual Authorization and Other Requirements for Research

Under the current Privacy Rule, a covered entity may condition the provision of treatment related to research on the individual's authorization to allow disclosure of his or her protected health information. A single or "compound" authorization document may be used in these circumstances to document both the individual's consent to participate in the research and for disclosure of his or her protected health information. However, where the research involves both research-related treatment and a corollary activity such as tissue banking, separate authorizations must be obtained. In response to concerns that the HIPAA Privacy Rule is inconsistent with other related laws and regulations that govern research activities (i.e., the Common Rule), HHS made two significant changes to research requirements under the Privacy Rule. First, HHS will now allow a covered entity to combine conditioned and unconditioned (i.e., for corollary activities) 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.[87] This change will apply to any type of research activities, not just clinical trials and biospecimen banking unless the research involves the use of psychotherapy notes in which case an authorization for use of psychotherapy notes may only be combined with another authorization for use of psychotherapy notes.[88]

This Rule continues to allow a covered entity to combine such authorizations with informed consent documents for the research studies and provides covered entities, institutions and Institutional Review Boards the flexibility to determine the best methods for differentiating between conditioned and unconditioned research activities and providing appropriate options to opt in to the unconditioned research activities. Importantly, the Final Rule does not eliminate the

[82] 45 C.F.R. § 164.520(b)(1)(iii)(A); 78 Fed. Reg. at 5624.
[83] 45 C.F.R. § 164.522(a)(1)(vi); 78 Fed. Reg. at 5624.
[84] 45 C.F.R. § 164.520(b)(1)(ii)(E); 78 Fed. Reg. at 5624.
[85] 45 CFR § 164.520(b)(1)(iii)(D).
[86] 45 CFR § 164.520; 78 Fed. Reg. at 5625.
[87] 45 CFR § 164.508(b)(3)(i) and (iii); 78 Fed. Reg. at 5610-11.
[88] 45 CFR § 164.508(b)(3)(ii).

requirement for an individual to authorize unconditioned research activities.[89]

Second, HHS also modifies the Department's prior interpretation and guidance that research authorizations must be research specific.[90] While this modification does not make any changes to the authorization requirements at 42 CFR § 164.508, HHS will no longer interpret the "purpose" provision as study specific thereby allowing future research to be authorized provide the authorization includes a description of the purpose of any future research.[91]

Modification to Individual Authorization and Other Requirements for Child Immunization Records

HHS finalized its proposal to permit a covered entity to disclose proof of immunization to a school where a state or other law requires the school to have such information prior to admitting the student without written authorization.[92] However, covered entities still must obtain agreement from the parent, guardian, person acting in loco parentis, or from the individual if an adult or emancipated. The covered entity must document the agreement, but HHS does not stipulate a standard for the documentation.[93] HHS also declined to define "school official" and "school" recognizing potential variation in state laws and types of schools that are subject to student entry laws.[94]

Decedent Health Information

Although the current Privacy Rule requires covered entities to protect a decedent's protected health information indefinitely, HHS finalized its proposal to require covered entities to comply with Privacy Rule requirements for the protected health information of a deceased individual for fifty years following date of death.[95] In addition, the Final Rule permits covered entities to disclose a decedent's information to family members and others involved in the decedent's care prior to death unless the decedent previously expressed otherwise.[96]

Additional Changes to Enforcement Rule (Not included in Interim Final Rule)

Formal Investigations: As required by HITECH, HHS finalized the provision requiring HHS to investigate any complaint or other source of information if it appears the possible violation was due to willful neglect and impose civil monetary penalties for violations dues to willful neglect

[89] 78 Fed. Reg. at 5610-11.
[90] 45 C.F.R. § 164.508(b)(3); 78 Fed. Reg. at 5612.
[91] 45 C.F.R. § 164.508(c) and § 164.508(c)(1)(iv).
[92] 45 C.F.R. § 164.512(b)(1).
[93] 45 C.F.R. § 164.512(b)(1); 78 Fed. Reg. at 5617.
[94] 78 Fed. Reg. at 5616.
[95] 45 C.F.R. § 164.502(f).
[96] 45 C.F.R. § 164.510(b)(5).

that are not cured within 30 days.[97]

Time to cure: HHS finalized its proposal 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 acquires actual or constructive knowledge of the violation and will be determined based on evidence gathered by HHS during its investigation, on a case-by-case basis.[98]

HHS Authority To Release Protected Health Information During an Investigation: Under existing HIPAA Rules, covered entities are required make information available to and cooperate with the HHS Secretary during the investigation of a complaint. HHS must not disclose any protected health information obtained during an investigation except as necessary for determining and enforcing compliance with HIPAA or as otherwise required by law. In the Final Rule, HHS finalized its proposal to also allow the HHS to disclose protected health information if permitted under the Privacy Act at 5 U.S.C. § 552a(b)(7) to better enable HHS to coordinate with other law enforcement agencies.[99] HHS provided the examples of State Attorneys General pursuing civil actions to enforce HIPAA on behalf of state residents pursuant to Section 13410(e) of the Act or the Federal Trade Commission pursuing remedies under other consumer protection authorities.[100]

Liability for Agents: HHS clarified that covered entities or business associates are liable for the acts of its agents acting within the scope of agency, whether the agents are workforce members or business associates.[101]

Affirmative Defenses: To conform to the changes made to Section 1176(b) of the Social Security Act by HITECH, HHS finalized its proposal that the affirmative defense of criminally "punishable" is applicable to penalties imposed prior to February 18, 2011, and on or after February 18, 2011.[102] The Secretary's authority to impose a civil money penalty will only be barred to the extent a covered entity or business associate can demonstrate that a criminal penalty has been imposed.[103] However, the prior definition of "reasonable cause" will still apply to violations occurring prior to February 18, 2009 to avoid any retroactive application of the revised term.[104]

[97] 45 C.F.R. § 160.312; 78 Fed. Reg. at 5577-79.
[98] 45 C.F.R. § 160.410(b)(2); 78 Fed. Reg. at 5579.
[99] 45 C.F.R. § 160.310(c)(3).
[100] 78 Fed. Reg. at 5579.
[101] 78 Fed. Reg. at 5580-81.
[102] 45 C.F.R. § 160.410(a)(1) and (2).
[103] 78 Fed. Reg. at 5582-83.
[104] 45 C.F.R. § 160.410.

Interaction with Patient Safety Quality Improvement Act: Penalties will not be imposed under both the Patient Safety Quality Improvement Act[105] and HIPAA Privacy Rule for the same violation.[106]

Additional Changes to the Privacy Rule

Patient Safety Activities: HHS finalized its proposal to include "patient safety activities" in the definition of "health care operations." This modification is intended to better align the requirements of the Patient Safety Quality Improvement Act with HIPAA.[107]

II. HIPAA Enforcement Rule

The Final Rule includes modifications to the HIPAA Enforcement Rules that were initially addressed in the Interim Final Rule issued in October 2009. Most significant of these are the changes to the liability determinations and associated penalties.[108]

Tiered Liability: The HITECH Act establishes tiered liability for HIPAA violations based on the level of culpability of a covered entity or business associate, using the terms "reasonable diligence," "reasonable cause," and "willful neglect" to describe increasing levels of culpability that correspond to increasing minimum penalties.[109] The statute did not amend the definition of these terms, which also were defined in the Interim Final Rule as follows:[110]

- *Reasonable Diligence.* The term refers to "the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances."
- *Reasonable Cause*. The term 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."
- *Willful Neglect.* The term refers to "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated."

Under HITECH, the lowest penalty 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 tier applies to violations due to reasonable cause and not willful neglect; the third tier applies to violations due to willful neglect that was corrected in a certain period of time, and the highest (fourth) tier applies to willful neglect that is not corrected.[111]

[105] 42 U.S.C. 299b–22(i).
[106] 45 C.F.R. § 160.418.
[107] 42 U.S.C. 299b–22(i).45 C.F.R. § 164.501; 78 Fed. Reg. at 5592.
[108] 78 Fed. Reg. at 5579-80.
[109] HITECH Act, § 13410(d).
[110] 45 C.F.R. §160.401; 74 Fed. Reg. at 56130.
[111] HITECH Act, § 13410(d).

In the Interim Final Rule, HHS moved the definitions of these three terms from the section pertaining to affirmative defenses to the section applying to the entirety of the Enforcement Rule and the imposition of civil monetary penalties.[112]

In the Final Rule, HHS finalizes its proposal to modify the definition of "reasonable cause," but not the other two terms.[113] HHS determined the modification is necessary to clarify the state of mind required for this category of violations, to ensure that all violations are captured by one of the three tiers. Specifically, HHS is changing 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."[114] HHS also includes examples and guidance for application of the three terms to distinguish among the tiers.[115]

Amount of Civil Monetary Penalty: 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.[116] The Interim Final Rule implemented the new penalty scheme for violations occurring on or after February 18, 2009. 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 of $1.5 million in yearly liability for identical violations; 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 of $1.5 million in yearly liability for identical violations; 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 of $ 1.5 million in yearly liability for identical violations; 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 of $1.5 million in yearly liability for identical violations.[117]

HHS finalizes its proposal 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.[118] Furthermore, HHS eliminates an affirmative defense that currently protects a

[112] 45 C.F.R. § 160.401; 74 Fed. Reg. at 56126.
[113] 45 C.F.R. § 160.408; 78 Fed. Reg. at 5580.
[114] 45 C.F.R. § 160.401; 78 Fed. Reg. at 5580.
[115] 78 Fed. Reg. at 5580-82.
[116] HITECH Act, § 13410(d).
[117] 74 Fed. Reg. at 56126.
[118] 45 C.F.R. §§ 160.404; 160.408; 160.410; 74 Fed. Reg. at 56126-29.

covered entity from liability for the actions of its business associate. 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.[119]

III. Breach Notification for Unsecured Protected Health Information

The requirements of the August 2009 Interim Final Rule for Breach[120] became effective on September 23, 2009.[121] This Final Rule largely maintains the provisions of the Interim Final Rule, but makes a few significant changes.

Harm Threshold: Most notably, the Final Rule replaces the Interim Final Rule's "harm" threshold with a more objective standard.[122] The Interim Final Rules define "breach" as the access, acquisition, use, or disclosure of protected health information in a way that violates the Privacy Rule and "compromises the security or privacy of the [information]."[123] Protected health information is compromised if there is a "significant risk of financial, reputational, or other harm to the individual."[124] Covered entities must conduct a risk assessment to determine whether the disclosure or use will result in a significant risk of harm to an individual (the "harm" standard).[125] HHS takes a much more objective approach in the Final Rule. First, HHS clarifies that an impermissible use or disclosures of protected health information is presumed to be a breach unless the covered entity can demonstrate that there is a low probability that the protected health information has been compromised.[126] Second, addressing significant concerns with the subjectivity of the "harm standard," HHS modified the standard to include a four-factor objective standard. Covered entities must now consider: 1) the nature and extent of protected health information involved, 2) the persons to whom disclosure was made, 3) whether the protected health information was actually acquired or viewed, and 4) the extent to which the risk of breach to the protected health information has been mitigated.[127]

Notification to the Media: The Interim Final Rule requires covered entities, upon discovering a breach of the protected health information of more than 500 individuals within a state or jurisdiction, to notify the media serving the applicable area without unreasonable delay but no later than 60 days after the discovery.[128] Media notices must contain the same information as is required for individual notifications in 42 CFR § 164.404(c).[129] In the Final Rule, HHS clarified that the regulation does not require media outlets to report information from covered entities and

[119] 45 C.F.R. § 160.408; 78 Fed. Reg. at 5583.
[120] 74 Fed. Reg. at 42740.
[121] 78 Fed. Reg. at 5568.
[122] 45 C.F.R. § 164.402; 78 Fed. Reg. at 5641-44.
[123] 74 Fed. Reg. at 42767-68.
[124] 74 Fed. Reg. at 42767-68.
[125] 74 Fed. Reg. at 42744.
[126] 45 C.F.R. § 164.402; 78 Fed. Reg. at 5641.
[127] 78 Fed. Reg. at 5642.
[128] 74 Fed. Reg. at 42768.
[129] 74 Fed. Reg. at 42768.

that posting a press release on the covered entity's website does not satisfy the notice requirement.[130]

Notification to the Secretary: The Interim Final Rule requires covered entities to notify HHS upon discovering a breach of unsecured protected health information.[131] If the breach involves more than 500 individuals, such notice must occur "contemporaneously" with the notice to individuals.[132] Covered entities must document breaches that affect fewer than 500 people and report these breaches to the HHS Secretary, in a form specified on the HHS website, within 60 calendar days of the end of the year in which the breaches occurred.[133] Responding to concerns from commenters about providing notice to the Secretary in the year following the "occurrence" of a breach, HHS amended the Interim Final Rules so that notification must occur within 60 days after the calendar year in which a breach is "discovered."[134] Commenters also urged HHS to permit covered entities to submit small breaches in log form rather than the current individual method.[135] HHS indicated that it recognizes individual submission is burdensome and is exploring alternative submission methods.[136]

Notification by a Business Associate: The HITECH Act requires business associates to notify a covered entity, without unreasonable delay and no later than 60 days, upon discovering a breach of unsecured protected health information.[137] In addition, the Interim Final Rule provides that covered entities discover a breach when their agent discovers it. Thus, the discovery of a breach by a business associate that is also an agent of a covered entity will automatically trigger the covered entity's breach notification obligations.[138] HHS indicated that it will issue additional guidance on the agent relationship in the future.[139]

IV. HIPAA Privacy Rule and GINA

In order to protect genetic information from being used to discriminate against individuals seeking insurance coverage, GINA requires genetic information to be treated as protected health information under the HIPAA Privacy Rule and prohibits four types of health plans (group health plans, health insurance issuers, HMOs, and issuers of Medicare supplemental policies) from using or disclosing genetic information for underwriting purposes.[140]

[130] 45 C.F.R. § 164.406; 78 Fed. Reg. at 5653.
[131] 45 C.R.F. § 164.408; 78 Fed. Reg. at 5653-54.
[132] 74 Fed. Reg. at 42768-69.
[133] 74 Fed. Reg. at 42753.
[134] 45 C.F.R. § 164.408(c); 78 Fed. Reg. at 5654.
[135] 78 Fed. Reg. at 5654.
[136] 78 Fed. Reg. at 5655.
[137] HITECH Act, § 13402(b); 78 Fed. Reg. at 5655-56.
[138] 45 C.F.R. § 164.410; 78 Fed. Reg. at 5656.
[139] 78 Fed. Reg. at 5656.
[140] GINA, § 105 (codified at 42 U.S.C. 1320d-9).

Prohibition Expanded to All Health Plans: In the proposed rule, HHS expanded the GINA requirements to prohibit all types of health plans (not just the four specified by GINA) subject to the Privacy Rule from using or disclosing protected health information that is genetic information for underwriting purposes.[141] HHS finalized this expanded application of GINA with the exception of issuers of long term care policies.[142] However, HHS makes clear that the prohibition on use or disclosure of protected health information that is genetic information for underwriting purposes is limited to health plans.[143] Providers may continue to disclose protected health information (including genetic information) to health plans for payment purposes where doing so meets the minimum necessary standard.[144] The health plan bears the burden not to use or disclose the protected health information it receives for prohibited underwriting purposes.[145] A provider may also continue to use or disclose genetic information as it sees fit for treatment of an individual.[146] Covered entities that are both a health plan and health care provider may use genetic information for treatment purposes, to determine the medical appropriateness of a benefit, and as otherwise permitted by the Privacy Rule, but may not use such genetic information for underwriting purposes.[147] Such covered entities should ensure that appropriate staff members are trained on the permissible uses of genetic information.

Definitions: The Final Rule also defines several terms, including "genetic information," "genetic test," "genetic services," "family member" and "manifestation and manifested."[148] However, HHS notes that it will issue future guidance on its website on the differences between genetic tests and medical tests,[149] and the Rule's protections for genetic information.[150] HHS also adopts the definition of underwriting purposes from GINA, which includes "activities related to the creation, renewal, or replacement of a contract of health insurance benefits."[151]

Interaction with Health Risk Assessments: A number of commenters raised concerns about health plans' ability to incentivize individuals to complete health risk assessments and participate in wellness programs.[152] While the Final Rule provides that such tools are permissible if their application does not involve the use or disclosure of genetic information,[153] it ultimately refuses to exclude these tools from the definition of underwriting purposes because GINA does not include an exception for wellness programs.[154]

---

[141] 78 Fed. Reg. at 5659- 60.
[142] 45 CFR § 164.502(a)(3); 78 Fed. Reg. at 5660-61.
[143] 78 Fed. Reg. at 5667).
[144] 45 CFR § 164.501; 78 Fed. Reg. at 5665, 5668.
[145] 45 CFR § 164.502(b)(1); 78 Fed. Reg. at 5668.
[146] 78 Fed. Reg. at 5667.
[147] 78 Fed. Reg. at 5667.
[148] 45 CFR § 160.103; 78 Fed. Reg. at 5662.
[149] 78 Fed. Reg. at 5662.
[150] 78 Fed. Reg. at 5664.
[151] 45 CFR § 164.502(a)(5)(i); 78 Fed. Reg. at 5665.
[152] 78 Fed. Reg. at 5665.
[153] 78 Fed. Reg. at 5665.
[154] 78 Fed. Reg. at 5665.

Interaction with other Payment and Health Care Operations Uses: The Final Rule also makes clear that health plans may not use or disclose protected health information that is genetic information for underwriting, even though such use or disclosure may be considered payment or health care operations.[155] However, HHS clarifies that a health plan may continue to use or disclose protected health information that is genetic information as required by law, except to the extent that doing so would be inconsistent with the prohibition against using or disclosing genetic information for underwriting purposes in GINA and the final rule.[156]

Notice of Privacy Practices: Finally, HHS requires health plans, except issuers of long-term care policies, that use or disclose protected health information for underwriting to include a statement in their Notice of Privacy Practices that they are prohibited from using or disclosing protected health information that is genetic information about an individual for such purposes.[157]

[155] 45 CFR § 164.506(a); 78 Fed. Reg. at 5667.
[156] 45 CFR § 164.514(g); 78 Fed. Reg. at 5667.
[157] 45 CFR § 164.520(b)(1)(iii)(D).