Bloomberg BNA

Health IT Law & Industry Report™

VOL. 0, NO. 0 JANUARY 23, 2013

BNA INSIGHTS

HIPAA Omnibus Rule Reshapes Landscape for Health Care Privacy, Security Compliance




BY ROBERT BELFORT, ANNE O'HAGEN KARL, KAREN Y. LAM, AND EMILY LEE

On Jan. 17, 2013, the Office for Civil Rights of the U.S. Department of Health and Human Services ("HHS") issued a long-awaited omnibus rule (the "Omnibus Rule"), which modifies a wide range of privacy, security and breach notification requirements under the Health Insurance Portability and Accountability Act ("HIPAA"). The Omnibus Rule, among other things:

- Replaces the controversial "risk of harm" standard for determining whether a reportable data breach has occurred with a new test focused on whether data have been "compromised."
- Extends the reach of HIPAA to business associates.
- Tightens restrictions on the use of protected health information ("PHI") for marketing purposes.
- Gives non-profit organizations greater leeway in using clinical information for fundraising.
- Provides greater flexibility for researchers seeking to obtain patient authorization for the use of PHI for research.
- Integrates protections governing genetic information established under other laws.
- Enhances patients' electronic access to their medical records.

Health care providers, health plans and other covered entities will have to revise their privacy and security policies, privacy notices and business associate con-

 ISSN 2151-2876

tracts to come into compliance. Subject to certain exceptions noted below, covered entities and business associates are required to comply with the Omnibus Rule by Sept. 23, 2013.

Regulatory History

The massive federal stimulus bill enacted in 2009 contained the Health Information for Economic and Clinical Health Act (''HITECH'').[1] While HITECH was focused, in part, on promoting the use of electronic health records, it also directed HHS to implement a wide variety of changes to the HIPAA Privacy Rule and Security Rule as well as a regulatory framework for breach notification. As required by HITECH, HHS issued an interim final rule governing breach notification on Aug. 24, 2009 (the ''Interim Breach Rule'').[2] HHS later indicated it was reconsidering certain aspects of the Interim Breach Rule. On July 14, 2010, HHS published a proposed rule addressing many of HITECH's privacy and security requirements (the ''Proposed Rule''). The Omnibus Rule revises the Interim Breach Rule and finalizes the Proposed Rule.[3]

The Omnibus Rule will be published in the *Federal Register* on Jan. 25, 2013, and will become effective on March 26, 2013. Covered entities and business associates will be required to comply with most of the provisions of the Omnibus Rule within 180 days of the effective date, which is Sept. 23, 2013.

Breach Notification

The Omnibus Rule replaces the Interim Breach Rule's controversial ''risk of harm'' standard with a requirement that covered entities treat improper disclosures of PHI as breaches unless they demonstrate there is a low probability the PHI was ''compromised.'' The Omnibus Rule largely retains the other provisions of the Interim Breach Rule relating to the timing and content of breach notices.

Modification of the Risk of Harm Standard

Under Section 13402 of HITECH, covered entities were required to notify affected individuals, HHS and, in some cases, the media, following the discovery of a breach of unsecured protected health information. The Omnibus Rule largely tracks the provisions of the Interim Breach Rule with one important exception: the controversial ''risk of harm'' standard has been replaced with a new obligation to assess whether PHI has been ''compromised.''

Under the Interim Breach Rule, a breach was defined as the unauthorized acquisition, access, use or disclosure of unsecured PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of the PHI. The Interim Breach Rule interpreted the phrase ''compromises the security or privacy of the PHI'' to mean an unauthorized use or disclosure that poses a significant risk of financial, reputational, or other harm to the individual. Covered entities were required under the Interim Final Rule to conduct a risk assessment to determine whether there was a significant risk of harm due to the impermissible use or disclosure.

The Omnibus Rule rejects the risk of harm test.[4] Instead, covered entities are now required to assess the risk that the PHI was ''compromised.'' The term ''compromised'' is not defined. But HHS indicates that, when conducting this assessment, the covered entity must consider at least the following factors: (1) the nature and extent of the PHI; (2) the unauthorized person who used or received the PHI; (3) whether the PHI was actually viewed or acquired; and (4) the extent to which the risk to the PHI has been mitigated.

It is somewhat unclear what the term ''compromised'' means in this context. The term ''compromised'' could mean ''improperly viewed or accessed,'' but this interpretation would be inconsistent with HHS commentary that there would be no breach under the new standard if a physician receives information about the wrong patient, identifies the error and returns the information to the covered entity. In that scenario, there would be improper viewing or access, but evidently no breach. And the factors specified for applying the new test are similar to those that had to be considered under the risk of harm standard.

Thus, while HHS's stated goal was to replace a subjective judgment about harm to the individual with a more objective assessment of whether the PHI was compromised, covered entities may still struggle in determining whether PHI has been compromised and a breach has occurred.

One clear change in the Omnibus Rule is that the burden of proof now rests on the covered entity. The covered entity must treat the incident as a breach unless, after considering the above factors, it determines there is a low probability the PHI was compromised.

Covered entities do not have to comply with the Omnibus Rule's new test until the Sept. 23, 2103, compliance date. Until then, the Interim Breach Rule's risk of harm standard will remain in effect.

Exceptions to the Definition of a Breach

The Interim Breach Rule established the following four exceptions to the definition of a breach:

- An impermissible use or disclosure of PHI that would qualify as a limited data set but also excludes dates of birth and zip codes does not constitute breach.
- A workforce member who unintentionally accesses or uses PHI in good faith does not trigger a breach.
- An inadvertent disclosure between two individuals authorized to access PHI at the same covered entity, business associate, or organized health care arrangement is not a breach.
- A disclosure where the covered entity has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the PHI is not a breach.

[1] Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), *codified at* 42 U.S.C. §§ 300jj *et seq.*; §§ 17901 *et seq.*

[2] 74 Fed. Reg. 42,740 (Aug. 24, 2009).

[3] HHS also issued a proposed HIPAA enforcement rule that is finalized in the Omnibus Rule. However, the enforcement provisions of the Omnibus Rule are outside the scope of this article. In addition, HHS issued a proposed rule on accountings of disclosures, but this proposed rule is not addressed in the Omnibus Rule and has been deferred for future rulemaking.

[4] 45 C.F.R. § 164.402.

  HITR ISSN 2151-2876

The Omnibus Rule does not adopt the above exception for limited data sets. But it incorporates the three other exceptions from the Interim Breach Rule.[5]

Notification Time Frames and Other Requirements

The Omnibus Rule implements without significant changes most of the other provisions of the Interim Breach Rule:

- Unsecured PHI is defined as PHI not secured through a technology or methodology specified by HHS. Thus, encrypting PHI in accordance with HHS standards continues to be the most effective step to prevent reportable breaches.
- Covered entities must notify each individual affected by a breach without unreasonable delay, but in no event more than 60 days after the date the breach was discovered or reasonably should have been discovered. A covered entity may delay notification, if such delay is requested by law enforcement. The notification must include specific information about the breach. The notice must be provided in writing and sent by first class mail or email (if the individual has generally requested communications by email). The covered entity may provide substitute notice, such as a posting on its website, if it lacks contact information for some individuals.
- Covered entities must notify prominent media outlets if the breach affects more than 500 individuals within a state. The notification to the media must be made within the same time frame and must include the same information as the notification to individuals.[6]
- Covered entities must notify HHS without unreasonable delay, but in no event longer than 60 days after discovery, of any breach of unsecured PHI of more than 500 individuals. For breaches affecting fewer than 500 individuals, the covered entity is required to log all such breaches and provide a copy of the log to HHS within sixty days after the end of the calendar year. As is currently the case, HHS will maintain a list on its website of all covered entities with breaches of unsecured PHI affecting more than 500 individuals.[7]
- A business associate must notify a covered entity of any breach without unreasonable delay, but in no event later than 60 days after the discovery of the breach. If the business associate is considered an agent of the covered entity under the federal common law of agency, then the covered entity is deemed to have discovered the breach when the business associate discovers it.[8]

Application of HIPAA to Business Associates

The Security Rule and certain provisions of the Privacy Rule now apply directly to business associates, who may be penalized by HHS for any violations. Business associates are defined more broadly than before to include any entities that maintain PHI on behalf of covered entities, HIOs, PSOs and subcontractors of first tier business associates. Business associate contracts must be amended to incorporate the Omnibus Rule's requirements by Sept. 23, 2013, although preexisting business associate contracts may remain in effect for one year thereafter.

Prior to HITECH, the HIPAA regulations did not directly apply to business associates and their subcontractors. While business associates could be subject to breach of contract claims by covered entities under their business associate contracts, they were not subject to civil (and arguably criminal) penalties under HIPAA.

HITECH significantly changed the way in which business associates are regulated under HIPAA. Section 13401 of HITECH provided that the Security Rule's requirement that covered entities maintain certain administrative, physical and technical safeguards applies to business associates in the same manner and to the same extent as covered entities. In addition, Section 13404 required business associates to adhere to the privacy requirements of their business associate contracts and HITECH's privacy provisions. Business associates may be subject to civil penalties and criminal liability for violations of these HITECH obligations.

The Proposed Rule implemented these changes by: (1) expanding the definition of the term ''business associate''; (2) making business associates directly liable for violations of the Security Rule and certain Privacy Rule requirements; and (3) clarifying the additional provisions that must be included in business associate contracts. The Omnibus Rule adopts these changes as proposed.

Broader Definition of "Business Associates"

The HIPAA regulations previously defined ''business associate'' generally to mean a person who performs specified functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of PHI. The Omnibus Rule expands the universe of business associates by including all entities that create, receive, maintain, or transmit PHI on behalf of a covered entity.[9]

As discussed below, the inclusion of the word ''maintain'' in this definition may impose HIPAA requirements on certain technology companies that previously have taken the position that they are not regulated under HIPAA. HHS notes that liability for impermissible uses and disclosures attaches once a person meets the definition of a business associate, without regard to whether the person has actually entered into a business associate contract.

HIOs and PSOs are Business Associates

Section 13408 of HITECH required certain data transmission vendors and personal health record vendors to be treated as business associates. The Final Rule expressly designates the following entities as business associates: Health Information Organizations, E-prescribing Gateways, or other person that provides data transmission services with respect to PHI to a covered entity and that require routine access to such PHI; and a person that offers a personal health record to one or more individuals on behalf of a covered entity.[10]

[5] 45 C.F.R. § 164.402.
[6] § 164.406.
[7] § 164.408.
[8] § 164.410.

[9] 45 C.F.R. § 160.103.
[10] 45 C.F.R. § 160.103. HHS declined to provide a definition for Health Information Organization, but intends to provide

Notably, HHS distinguishes vendors that *transmit* PHI from vendors that *maintain* PHI on behalf of covered entities. The former are business associates only if they routinely access PHI; if not, they are ''conduits,'' such as internet service providers, that are outside the scope of HIPAA.

In contrast, vendors that maintain PHI are business associates even if they do not require routine access to the PHI. This interpretation would appear to impose HIPAA requirements on certain cloud computing companies and other data storage vendors that previously took the position they were not business associates.

The Omnibus Rule also provides that the performance of patient safety activities gives rise to a business associate relationship.[11] Thus, patient safety organizations performing services under the Patient Safety and Quality Improvement Act are now business associates.

Subcontractors are Defined as Business Associates

Previously, a business associate was defined as an entity that performed certain functions for or on behalf of a covered entity. Subcontractors of business associates were not deemed business associates themselves. The Omnibus Rule changes that framework by providing that a business associate also includes ''a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.''[12]

As a result, subcontractors all the way down the contractual chain from covered entities have the same compliance obligations under HIPAA.

New Privacy and Security Rule Obligations of Business Associates

As required by HITECH and set forth in the Proposed Rule, the Omnibus Rule applies certain Privacy Rule provisions directly to business associates. Under the Omnibus Rule:

- A business associate, like a covered entity, may not use or disclose PHI except as permitted or required by the Privacy Rule.[13]
- A business associate may use or disclose PHI only as permitted or required by its business associate contract or as required by law.
- A business associate may not use or disclose PHI in a manner that would violate the requirements of the Privacy Rule if done by the covered entity, except for the proper management and administration of the business associate and data aggregation services, if such uses and disclosures are permitted under its business associate contract.[14]
- Business associates are directly liable for failing to enter into business associate agreements with subcontractors that create or receive PHI on their behalf.[15]
- A business associate must disclose PHI when required by HHS for HHS to investigate and determine the business associate's compliance with HIPAA
- A business associate must disclose PHI to the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations with respect to an individual's request for an electronic copy of PHI.[16]

In accordance with HITECH § 13405(b), the Omnibus Rule also clarifies that a business associate is subject to HIPAA's ''minimum necessary'' rule. When using or disclosing PHI or when requesting PHI from another covered entity or business associate, business associates must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.[17]

To implement Section 13401 of HITECH, the Omnibus Rule amends the Security Rule to make clear that business associates, like covered entities, must implement administrative, physical, and technical safeguards and policies to secure electronic PHI, and comply with HIPAA's policies and procedures and documentation requirements.[18]

Thus, business associates are directly responsible for conducting a risk analysis, implementing a security awareness and training program, appointing a Security Officer, and entering into business associate contracts with subcontractors, among other requirements.

As a result of these changes, HHS notes that a business associate is now directly liable for: impermissible uses and disclosures; a failure to provide breach notification to the covered entity; a failure to provide access to a copy of electronic PHI to either the covered entity, the individual, or the individual's designee (whichever is specified in the business associate contract); a failure to disclose PHI where required by HHS to investigate or determine the business associate's compliance with HIPAA; a failure to provide an accounting of disclosures and a failure to comply with the Security Rule.[19]

Changes to Business Associate Contracts

HIPAA permits a covered entity to disclose PHI to a business associate and to allow a business associate to create and receive PHI on its behalf, if the covered entity obtains satisfactory assurances in writing (in the form of a business associate or other agreement) that the business associate will appropriately safeguard the information.[20]

The Omnibus Rule modifies the business associate contract provisions to specifically require the business associate to comply with the Security Rule safeguards for electronic PHI, report breaches of unsecured PHI to covered entities as required under the breach notification rule, and to ensure any subcontractors that receive,

---

further guidance in this area as electronic health information exchange continues to evolve.

[11] *Id.*

[12] *Id.*

[13] 45 C.F.R. § 164.502(a).

[14] 45 C.F.R. § 164.502(a)(3).

[15] 45 C.F.R. § 164.502(e)(1)(ii).

[16] 45 C.F.R. § 164.502(a)(4). Section 13405(e) of HITECH requires covered entities that maintain PHI in an electronic health record to provide an individual with a copy of such information in an electronic format, if the individual chooses. The Omnibus Rule applies a similar requirement directly on business associates.

[17] 45 C.F.R. § 164.502(b). HHS intends to issue future guidance on the minimum necessary standard.

[18] 45 C.F.R. Part 160, and Part 164, Subparts A and C.

[19] HITECH § 13405; 76 Fed. Reg. 31426 (May 31, 2011).

[20] 45 C.F.R. § 164.502(e).

  HITR ISSN 2151-2876

create, maintain, or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate.[21]

Moreover, the agreement must require that if the business associate carries out a covered entity's obligation under the Privacy Rule, the business associate must comply with the Privacy Rule requirements that would apply to the covered entity in the performance of this obligation.[22]

Under HIPAA, a covered entity that knows of a material breach or violation by the business associate of its obligation under the agreement must take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, terminate the contract or report the problem to HHS (if termination is not feasible). In light of the direct liability imposed on business associates, the Omnibus Rule removes the requirement that covered entities report to HHS if termination is not feasible.[23]

The Omnibus Rule also adds a new, parallel provision for business associates and their subcontractors, requiring a business associate that is aware of noncompliance by its subcontractor to respond in a similar manner.[24]

A business associate must enter into similar agreements with subcontractors that create, receive, maintain, or transmit PHI on the business associate's behalf.[25] The requirements above for contracts between covered entities and business associates also apply to the contract between a business associate and their subcontractors.[26] The Omnibus Rule clarifies that a covered entity is not required to enter into business associate contracts with subcontractors of business associates, as this obligation is imposed on business associates.[27]

The Omnibus Rule provides for a one-year extension beyond the otherwise applicable compliance date for covered entities and business associates (or business associates and subcontractors) to revise their business associate contracts if such contracts were entered into and compliant with HIPAA as of Jan. 25, 2013.[28]

If the parties have a compliant contract in place before Jan. 25, 2013, and the contract is not renewed between March 26, 2013 and Sept. 23, 2013 (the standard compliance date), then the parties may rely on that contract until Sept. 22, 2014. If the parties do not have a compliant contract in place by Jan. 25, 2013, the parties will need to enter into a compliant agreement a year earlier, or by Sept. 23, 2013.

Use of PHI for Marketing

The Omnibus Rule prohibits covered entities from using PHI to send promotional communications paid for by third parties, except for refill reminders for which the covered entity receives a cost-based fee.

The Privacy Rule generally prohibits the use or disclosure of PHI for marketing purposes without the individual's authorization. The Privacy Rule previously excluded from the definition of marketing uses or disclosures of PHI (i) for treatment by a health care provider, (ii) to describe a health-related product or service that is provided by, or included in a plan of benefits, of the covered entity making the communication or (iii) for case management, care coordination, contacting individuals about treatment alternatives or related activities that do not constitute treatment.[29] Prior to the Omnibus Rule, it was immaterial whether a covered entity was receiving payment from a third party for making the communication if it fit within one of these exceptions.

HITECH significantly changed that framework. Under the Omnibus Rule, the activities noted above all constitute marketing if the covered entity receives payment from a third party for making the communication.[30]

The Omnibus Rule clarifies that in order to lose the benefit of these exceptions, the covered entity must receive payment from the party whose products or services are being promoted. For example, a hospital cannot use PHI to notify patients about the acquisition of a new piece of equipment if the communication is paid for by the equipment's manufacturer. But payment by a community foundation would be permissible.

The Omnibus Rule also states that the exceptions are unavailable only if the third party actually pays the covered entity for the communication; the provision of in-kind support such as brochures is not prohibited.

The Omnibus Rule contains one important exception to the prohibition on subsidized promotional communications. Refill reminders, which include communications about a drug or biologic currently prescribed to the individual or a generic substitute, may be paid for by third parties if the payment reasonably relates to the cost of the communication.

Significantly, a provision in the Proposed Rule that permitted subsidized promotional communications for other treatment purposes was *not* included in the Omnibus Rule. Thus, a pharmacy may receive payment from a pharmaceutical manufacturer to remind customers to refill their existing prescriptions or suggest they contact their doctor about a generic alternative, but pharmacies cannot receive such payment to recommend a switch from one brand name drug to another.

Sale of PHI

The Omnibus Rule tracks HITECH by prohibiting the sale of PHI, except for certain purposes and, in some cases, subject to a reasonable cost cap on fees.

Subject to certain exceptions, HITECH prohibited the sale of PHI. The Omnibus Rule largely adopts the provisions in the Proposed Rule implementing this prohibition.[31]

The Omnibus Rule defines the ''sale of PHI'' as the exchange of remuneration (i.e., anything of value) in return for PHI. A sale does not have to involve a transfer of ownership of the PHI and may include licensing or other arrangements under which access to PHI is facili-

[21] 45 C.F.R. § 164.504(e)(2)(ii)(B) through (D).

[22] 45 C.F.R. § 164.504(e)(2)(ii)(H). For example, if a third party administrator of a group health plan fails to distribute the plan's notice of privacy practices on a timely basis, the vendor would be contractually liable for the failure. The covered entity would also remain directly liable under HIPAA for failure to provide the notice.

[23] 45 C.F.R. § 164.504(e)(1)(ii).

[24] 45 C.F.R. § 164.504(e)(1)(iii).

[25] 45 C.F.R. § 164.502(e)(1)(ii).

[26] 45 C.F.R. § 164.504(e)(5) and 164.502(e)(1)(ii).

[27] 45 C.F.R. §§ 164.308(b)(1) and 164.502(e)(1)(i).

[28] 45 C.F.R. § 164.523.

[29] 45 C.F.R. § 164.501.

[30] *Id.*

[31] 45 C.F.R. § 164.502(a)(5)(ii).

tated. But payment for services such as those of health information exchange does not constitute the sale of PHI.

The Omnibus Rule tracks the exceptions to the prohibition on the sale of PHI contained in HITECH and the Proposed Rule that permit the exchange of remuneration for disclosure of PHI:

- For public health purposes.
- For research purposes if the remuneration is limited to a fee equal to the direct and indirect costs incurred by the covered entity in preparing and transmitting the PHI.
- For treatment and payment purposes.
- For the sale, transfer, merger or consolidation of the covered entity's business.
- To or by a business associate for activities undertaken on behalf of a covered entity if the only remuneration is payment by the covered entity for the business associate's services.
- To an individual requesting access to his or her PHI as restricted by the Privacy Rule.
- As required by law.
- For any other purpose permitted by the Privacy Rule if the only remuneration is a fee equal to the cost of preparing and transmitting the PHI.

Use of PHI for Fundraising

Not-for-profit health care organizations can now use information about the department in which the patient received services and the identity of the treating physician to target fundraising communications. But they must comply with stricter requirements to ensure that patients can exercise their right to opt out of future fundraising appeals.

Hospitals and other not-for-profit health care providers have long struggled under HIPAA to target their fundraising appeals to patients based on the nature of the services received by the patient from the provider. The Omnibus Rule gives them new flexibility to do so.[32]

Previously, the Privacy Rule permitted covered entities to use only demographic information (e.g., name, address, telephone number), insurance status and dates of service for purposes of developing fundraising communications. The use of any clinical information was prohibited. Under the Omnibus Rule, covered entities are now permitted to also use:

- General information about the department in which the patient was served (e.g., oncology, orthopedics, etc.).
- The identity of the patient's treating physician.
- General outcome information (e.g., patient death or sub-optimal result).

This flexibility will allow cover entities to target fundraising based on a patient's potential interest in a particular clinical initiative (e.g., asking patients treated for cancer to support a new cancer center). It will also enable providers to send fundraising appeals under the name of the patient's physician.

Covered entities sending fundraising communications have always been required to notify patients of their right to opt out of future fundraising appeals. But under the Omnibus Rule, as required by HITECH, this notice must now be ''clear and conspicuous.''

The Omnibus Rule also adopts language in the Proposed Rule requiring covered entities to provide an opt out mechanism that does not impose an ''undue burden'' on patients. HHS indicates that obligating patients to send a letter would constitute an undue burden but offering them a telephone number or a self-addressed, stamped postcard would not. Opt outs may be specific to a particular fundraising appeal or broad enough to cover all appeals, at the discretion of the covered entity.

Finally, the Omnibus Rule requires covered entities to honor all opt outs, rather than merely using reasonable efforts to do so as previously required by the Privacy Rule.

Use of PHI for Research

The Omnibus Rule simplifies the process of obtaining patient authorization for research by permitting a single authorization form to combine ''conditioned'' and ''non-conditioned'' research, and by providing flexibility to obtain a single authorization for multiple research projects.

The Privacy Rule generally prohibits covered entities from conditioning treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of an authorization to use or disclose PHI.[33] However, there is an important exception that allows a covered entity to condition the provision of research-related treatment (e.g., treatment in a clinical trial) on obtaining an individual's authorization for the disclosure of their PHI in connection with such research.[34] The exception does not apply, though, to retrospective research that is not performed as a part of a treatment regimen.

Previously, an authorization for ''conditioned'' research (i.e., research performed in connection with a clinical trial or other treatment) could not be combined with an authorization for ''unconditioned'' research (i.e., retrospective research unrelated to treatment). This limitation required researchers to obtain separate authorizations when conducting clinical trials associated with corollary research activities such as collecting specimens for a central repository.

In response to complaints from researchers about the burden of obtaining multiple authorizations, the Proposed Rule allowed a covered entity to combine conditioned and unconditioned research authorizations so long as the combined authorization clearly differentiated between the conditioned and unconditioned research components and clearly allowed the participant the option to opt into the unconditioned research components.[35] The Omnibus Rule adopts this modification, subject to one limitation: an authorization for use or disclosure of psychotherapy notes in connection with research may only be combined with another authorization for use or disclosure of psychotherapy notes.[36]

The Omnibus Rule also modifies HHS's prior interpretation of the Privacy Rule that research authoriza-

[32] 45 C.F.R. § 164.514(f).

[33] 45 C.F.R. § 164.508(b)(4).
[34] 45 C.F.R. § 164.508(b)(4)(i).
[35] 45 C.F.R. § 164.508(b)(3)(i).
[36] *See* 45 C.F.R. § 164.508(b)(3)(ii).

  HITR ISSN 2151-2876

tions must be study specific.[37] Researchers complained that this restriction impeded future research that could not be identified at the time the initial authorization was obtained.

In response, HHS indicated in the Proposed Rule that it was considering a number of options regarding authorizations for future research. Under the Omnibus Rule, HHS modified its interpretation, allowing authorizations to either be study-specific or broad enough to encompass a range of future research projects, as long as the authorization adequately describes such research. HHS declined to prescribe specific statements that must included in such an authorization.

Use of Genetic Information

The Omnibus Rule incorporates genetic information into the definition of PHI and conforms the Privacy Rule to federal laws restricting the use of such information by barring all health plans other than long term care insurers from using genetic information for underwriting purposes.

The Genetic Information Nondiscrimination Act of 2008 (''GINA'') prohibits discrimination based on an individual's genetic information in both the health coverage and employment contexts.[38] In addition to these nondiscrimination provisions, Section 105 of Title I of GINA contains privacy protections for genetic information and requires modification of the Privacy Rule to: (1) clarify that genetic information is health information; and (2) prohibit group health plans, health insurance issuers (including HMOs) and issuers of Medicare supplemental policies from using or disclosing genetic information for underwriting purposes. As required by GINA, on October 7, 2009, HHS published a proposed rule to strengthen privacy protections for genetic information as required by GINA (the ''GINA Proposed Rule''). The Omnibus Rule finalizes and implements these modifications.

In particular, under the GINA Proposed Rule, health plans ''shall not use or disclose protected health information that is genetic information for underwriting purposes.''[39] HHS applied these prohibitions to *all* health plans subject to the Privacy Rule (rather than to the more limited plans specified in GINA). The Omnibus Rule generally adopts this approach but exempts long-term care insurers.

GINA defined ''underwriting purposes'' to mean: (1) rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy; (2) the computation of premium or contribution amounts under the plan, coverage, or policy; (3) the application of any pre-existing condition exclusion under the plan, coverage, or policy; and (4) other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.[40]

The GINA Proposed Rule incorporated this statutory definition into the Privacy Rule and added certain clarifications consistent with the applicable implementing regulations for GINA.[41] For example, changes in cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program were included are permissible.[42] The GINA Proposed Rule also clarified that the underwriting does not include determinations of medical appropriateness where an individual seeks a benefit under a plan.[43] The Omnibus Rule adopts theses provisions from the GINA Proposed Rule.[44]

The Omnibus Rule also adopts the GINA Proposed Rule's provisions to explicitly include ''genetic information'' within the definition of PHI and make certain technical corrections to the Privacy Rule.[45] Finally, as discussed below, the Omnibus Rule revises certain provisions relating to the Notice of Privacy Practices (''NPPs'') for health plans that perform underwriting.

PHI of Decedents

PHI loses HIPAA protection 50 years after the individual's death. Covered entities may disclose PHI to a deceased individual's family members as long as the disclosure is not inconsistent with the prior expressed preferences of the individual.

Previously, the Privacy Rule required covered entities to protect the privacy of decedents' PHI to the same extent as the PHI of living individuals. For disclosures requiring authorization under the Privacy Rule, the covered entity needed to obtain the authorization from the decedent's personal representative, i.e., the executor or administrator of the decedent's estate.[46]

In response to comments from archivists and historians eager to access the information contained in the historical records of covered entities, the Proposed Rule redefined PHI to exclude information about individuals who have been deceased for at least 50 years. The Omnibus Rule adopts this new definition.[47] As a result, covered entities may (but are not required to) use or disclose the PHI of individuals who have been deceased for 50 or more years for any purpose. The Omnibus Rule also clarifies that covered entities are not required to retain records for fifty years.

The Omnibus Rule also addresses another complaint raised about the PHI of decedents. Previously, the Privacy Rule stated that only a decedent's personal representative could authorize disclosures of PHI.[48] As a result, family members who were able to obtain information about an individual's care while the individual was alive were no longer able to obtain similar information after the individual's death if they were not the executor or administrator of the individual's estate. The Proposed Rule permitted covered entities to disclose information about a decedent to family members or others involved in his or her care or payment for treatment, unless such disclosures would be inconsistent with the prior expressed preference of the individual. Family members are defined to include dependents and first degree, second degree, third degree and fourth degree relatives of the individual or his or her dependents.[49] The Omnibus Rule adopts this provision without modification.

---

[37] 45 C.F.R. § 164.508(c)(1)(iv).
[38] Pub. L. 110–233, 122 Stat. 881.
[39] 45 C.F.R. § 164.502(a)(5)(i).
[40] GINA § 105.
[41] *See* 45 C.F.R. § 164.502(a)(5)(i).
[42] 45 C.F.R. § 164.502(a)(5)(i)(A)(1).
[43] 45 C.F.R. § 164.502(a)(5)(i)(B).
[44] *See* 45 C.F.R. §§ 164.502(a)(5)(i)(A)-(B).
[45] *See* 45 C.F.R. § 160.103.
[46] § 164.502(f).
[47] § 164.502(f).
[48] § 164.510(b).
[49] 45 C.F.R. § 160.103.

Individuals' Access to PHI in Electronic Form

The Omnibus Rule requires covered entities to provide an individual with an electronic copy of his or her PHI if the PHI is maintained in any electronic designated record set, including but not limited to, an electronic health record (''EHR'').

The Privacy Rule establishes, with certain exceptions, a right for individuals to inspect or obtain copies of their PHI to the extent such information is maintained in the designated record set of a covered entity. In connection with such a request, the covered entity may impose a ''reasonable, cost-based fee.''[50]

Section 13405(e) of HITECH strengthened the Privacy Rule's right of access with respect to covered entities that use or maintain an EHR.[51] HITECH granted individuals the right to obtain an *electronic* copy of any PHI maintained in an EHR.[52] Fees were limited to the covered entity's labor costs in responding to the request.

The Proposed Rule expanded this HITECH provision beyond EHRs to cover any PHI ''maintained in one or more designated record sets electronically.''[53] Where the electronic information is not readily producible in the form and format requested, the information must be provided in an alternative readable electronic form and format as agreed to by the covered entity and the individual.[54] The Omnibus Rule adopts this provision.

With respect to the reasonable cost-based fee, the Omnibus Rule adopts the Proposed Rule's modifications to identify separately the labor costs for copying PHI from the supply costs associated with creating the electronic copy.[55] The Omnibus Rule also clarifies that a covered entity may charge for postage where the individual requests that the portable media containing the electronic copy be transmitted via mail or courier. Covered entities may *not* include fees associated with maintaining systems, retrieval costs or infrastructure costs.

The Omnibus Rule also modifies the Privacy Rule with respect to timely action by a covered entity in response to a request for access to off-site records.[56] Previously, the standard 30-day time frame for responding to access requests could be extended for another 30 days if the records were only accessible from an off-site location. The Proposed Rule requested comments on this provision and the Omnibus Rule modifies the Privacy Rule by removing the additional 30-day extension for off-site records.

Restrictions on Disclosures Requested by Patients

The Omnibus Rule implements the HITECH provision requiring covered health care providers to agree to a request by a patient that his or her PHI not be disclosed to a health plan for payment or health care operations if the PHI pertains solely to items or services for which the patient paid the provider out of pocket in full and the disclosure is not required by law.

Previously, the Privacy Rule required covered entities to maintain a process under which individuals could request restrictions on uses or disclosures of PHI for the purposes of treatment, payment, and health care operations, as well as disclosures to family members.[57] However, covered entities were not required to agree to any requested restriction.

HITECH created an exception to the general rule that covered entities have discretion regarding restriction requests. Under HITECH, health care providers were required to agree to a request by a patient that his or her PHI not be disclosed to a health plan for payment or health care operations if the PHI pertains solely to items or services for which the patient paid the provider out of pocket in full and the disclosure is not required by law. The Proposed Rule implemented this exception, clarifying that a covered entity is prohibited from making such disclosures to a business associate of the health plan, but the covered entity may disclose the PHI to its own business associate for other purposes. The Omnibus Rule implements this provision without modification.[58]

The Omnibus Rule clarifies that covered health care providers are not required to create separate medical records or otherwise segregate the PHI subject to this restriction as long as they prevent its disclosure. The Omnibus Rule also clarifies that providers may unbundle billing for items or services to accommodate an individual's restriction request, but they must first counsel the individual that the health plan may be able to determine the other services that were provided from such claims. In addition, providers are not required to notify downstream providers of the restriction. Finally, the Omnibus Rule provides guidance that payments from a health savings account or flexible spending account constitute payment on behalf of the individual.

Changes to Privacy Notices

The Omnibus Rule requires that various new provisions be included in NPPs. As a result, covered entities will have to modify their NPPs and redistribute them as required by the Privacy Rule.

Under the Privacy Rule, a covered entity must include separate statements about permitted uses and disclosures of PHI that the covered entity intends to make, including uses and disclosures for certain treatment, payment or health care operations purposes.[59] Prior to the Omnibus Rule, the NPP had to contain a statement that any uses and disclosures other than those permitted by the Privacy Rule would only be made with the individual's written authorization and that the individual had the right to revoke an authorization.[60] The Omnibus Rule adopts the Proposed Rule's modifications to this requirement to require that the NPP include an express statement that: (1) most uses and disclosures of psychotherapy notes and of PHI for marketing purposes and the sale of PHI require an individual's authorization; and (2) uses and disclosures not described in the NPP will be made only with the individual's authorization.

The Privacy Rule has historically required a covered entity to include separate statements in the NPP where it intends to: (1) contact individuals to provide appointment reminders or information about treatment alternatives or other health-related benefits or services; (2)

[50] 45 C.F.R. § 164.524.
[51] HITECH § 13405(e).
[52] HITECH § 13405(e)(1).
[53] 45 C.F.R. § 164.524(c)(2)(ii).
[54] *Id.*
[55] 45 C.F.R. §§ 164.524(c)(4)(i)-(ii).
[56] *See* 45 C.F.R. § 164.524(b).
[57] § 164.522(a).
[58] § 164.522(a).
[59] 45 C.F.R. § 164.520 (b)(1)(ii).
[60] 45 C.F.R. § 164.520(b)(1)(ii)(E).

  HITR ISSN 2151-2876

to contact the individual to fundraise for the covered entity; or (3) with respect to a group health plan, to disclose PHI to the plan sponsor.

The Proposed Rule modified the first requirement related to appointment reminders to better align it with the other proposed modifications relating to marketing and subsidized treatment communications. The Proposed Rule also modified the second requirement above related to fundraising to additionally provide for an individual's right to opt out of receiving fundraising communications. Because, as discussed above, the Omnibus Rule treats all subsidized treatment communications (other than refill reminders) as marketing communications, the former proposal was not adopted. The Omnibus Rule adopted the latter modification with regard to fundraising.[61]

The Omnibus Rule adopts the provision of the Proposed Rule requiring NPPs to explain that a covered entity is required to agree to a request to restrict disclosure of PHI to a health plan where the disclosure is for payment or health care operations and pertains to a health care item or service for which the individual has paid out of pocket in full.[62] The Omnibus Rule also requires covered entities to include in their NPP a statement of the right of affected individuals to be notified following a breach of unsecured PHI.[63]

The Proposed Rule indicated that the aforementioned modifications would constitute material revisions to covered entities' NPPs. Taking into consideration the potential burden on health plans, the Proposed Rule presented a couple of options with regard to the appropriate manner for informing individuals in a timely manner of material revisions to NPPs. The Omnibus Rule ultimately adopts an approach where a health plan that posts its NPP on its website must prominently post the change or a revised NPP on the website by the effective date of the change along with providing the revised NPP (or information about the change and how to obtain the revised NPP) in its next annual mailing to members.[64] Where a health plan does not post its NPP on its website, the health plan must provide the revised NPP (or information about the material change and how to obtain the revised NPP) to individuals within 60 days of the change.[65] Health care providers must comply with the standard Privacy Rule provision requiring them to make a modified NPP available to patients at its facilities upon request and post the revised NPP at such locations.

Finally, as noted above, the Omnibus Rule requires health plans that use or disclose PHI for underwriting to include a statement in their NPP that they are prohibited from using or disclosing genetic information for such purposes.[66]

Requirements for Hybrid Entities

Hybrid entities must include all business associate-type functions within their health care component for HIPAA compliance purposes.

The hybrid entity provisions of HIPAA permit a covered entity to limit HIPAA's application to the entity's components that perform functions that would make the component a covered entity if the component were a separate legal entity. In such a case, most of the HIPAA requirements apply only to the designated health care component of the entity. Prior to the Omnibus Rule, hybrid entities had the flexibility to either include or exclude their centralized components performing business associate-type functions (e.g., legal, human resources, information technology) from their health care component.

Under HITECH and the Omnibus Rule, business associates are separately and directly liable for violations of the Security Rule and for violations of the Privacy Rule for impermissible uses and disclosures. A hybrid entity could avoid direct liability and obligations for its business associate-type functions by not including these functions within the health care component. To address this concern, the Proposed Rule required a covered entity that is a hybrid entity to include a component that performs business associate-like activities within its health care component. The Omnibus Rule adopts this proposal.[67] HHS also adopted proposed changes clarifying that the entire covered entity, and not merely its health care component, remains responsible for complying with the business associate arrangements and other organizational requirements of HIPAA.[68]

---

[61] 45 C.F.R. § 164.520(b)(1)(iii)(B).

[62] 45 C.F.R. § 164.520(b)(1)(iv)(A). *See also* 45 C.F.R. § 164.522(a)(1)(vi).

[63] 45 C.F.R. § 164.520(b)(1)(v)(A).

[64] 45 C.F.R. § 164.520(c)(2)(v)(A).

[65] 45 C.F.R. § 164.520(c)(2)(v)(B).

[66] 45 C.F.R. § 164.520(b)(1)(iii)(C).

[67] 45 C.F.R. § 164.105(a)(2)(ii).

[68] 45 C.F.R. § 164.105(a)(2)(iii)(C).

   ISSN 2151-2876