Bloomberg BNA

BNA's
Health Law Reporter™

Health Information

The Department of Health Human Services Office for Civil Rights recently published its long-awaited final omnibus Health Insurance Portability and Accountability Act rule. The authors provide a comprehensive review of the final rule, which embodies four separate privacy, security, enforcement, and data breach rules. The primary thrust of the final rule, the authors write, is the expansion of HIPAA's regulatory authority to business associates and their subcontractors.

Final HIPAA Omnibus Rule Brings Sweeping Changes to Health Care Privacy Law: HIPAA Privacy and Security Obligations Extended to Business Associates and Subcontractors

BY REECE HIRSCH AND HEATHER DEIXLER

On Jan. 25, the Office for Civil Rights (OCR) of the Department of Health & Human Services (HHS) published the long-anticipated final rule (the Final Rule)[1] modifying the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and implementing the most significant changes to health care privacy law in a decade. The Final Rule amends the HIPAA privacy, security, enforcement, and breach notification rules pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act, and makes changes consistent with the Genetic Information Nondiscrimination Act of 2008 (GINA) (12 HLR 123, 1/28/13). The Final Rule, which becomes effective March 26, 2013, with compliance required by Sept. 23, 2013, dramatically expands the reach of HIPAA from its original focus on covered entities (health care providers, health plans, and health care clearinghouses) to a vast array of ''business associates'' to those covered entities and their subcontractors.

With a few notable exceptions, such as security breach notification and marketing, the Final Rule implements the proposed rule published July 14, 2010 (the Proposed Rule) without major modifications. Except as expressly noted below, the Final Rule implements the Proposed Rule without changes. However, in responding to comments on the Proposed Rule, OCR offers new guidance on many interpretive issues under HIPAA.

Reece Hirsch is a partner and Heather Deixler is an associate in the San Francisco office of Morgan, Lewis & Bockius LLP. They can be reached at (415) 442-1422, rhirsch@morganlewis.com, or hdeixler@morganlewis.com.

[1] 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 (Jan. 25, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

 ISSN 1064-2137

The primary thrust of the Final Rule is the expansion of HIPAA's regulatory authority to business associates and their subcontractors. These new obligations are a corollary to the HITECH Act's incentives promoting the adoption of electronic health records (EHRs). OCR seems to recognize that medical information is increasingly used and disclosed by an enormous variety of companies, some of them innovative and relatively new on the scene (health information exchanges, EHR vendors, and personal health record (PHR) companies) and some familiar players in the industry (billing, repricing, and management companies)—but none of them directly regulated under the current HIPAA privacy and security rules (the Privacy Rule and Security Rule). The Final Rule seeks to enhance consumer confidence in EHRs and other processes involving protected health information (PHI) by extending HIPAA privacy and security obligations to apply to these vendors. The Final Rule promises to stir a flurry of activity in the health care industry as business associates, along with all of their downstream subcontractors receiving PHI, prepare to comply with the Final Rule's standards by Sept. 23, or risk newly enhanced HIPAA sanctions.

Business Associates

Like the HITECH Act and the Proposed Rule, the Final Rule imposes new privacy and security obligations on business associates, starting with the definition of the term ''business associate.''

Expansion of the Definition of Business Associate

The Final Rule adds the following to the ''business associate'' definition:[2]

- ''patient safety organizations,'' which are organizations that conduct patient safety and quality improvement activities under the Patient Safety and Quality Improvement Act of 2005 (PSQIA) (This provision conforms HIPAA with the requirements of the PSQIA.);
- organizations that provide data transmission of PHI to a covered entity, such as health information organizations and e-prescribing gateways, and that require routine access to PHI (OCR reaffirms that ''mere conduits'' that do not access PHI, except on a random or infrequent basis, are not business associates.);
- vendors offering a PHR to one or more individuals on behalf of a covered entity; and
- subcontractors to a business associate that create, receive, maintain, or transmit PHI on behalf of a business associate.

The expansion of the definition of ''business associate'' to include subcontractors is one of the most significant features of the Final Rule, and was not addressed in the HITECH Act. OCR states that the intent of the provision is to ensure that privacy and security protections for PHI do not lapse simply because a function is performed by a ''downstream entity'' that has no direct contractual relationship with a covered entity.[3] Subcontractors would be subject to Privacy Rule and Security Rule obligations to the same degree as a business associate, and would be directly liable for violations. In order to clarify the scope of this expansion, OCR added a new definition of ''subcontractor'' in the Final Rule.[4]

OCR notes that the ''conduit'' exception is limited to services that transmit PHI, even when there is temporary storage of the transmitted data incident to the transmission.[5] However, a company that maintains PHI on behalf of a covered entity, such as a data storage company, is a business associate, even if the entity does not actually view the PHI. This distinction between ''transient'' and ''persistent'' access to PHI is a fine one, but it will determine whether certain companies are business associates. In order to clarify this point, OCR modified the definition of ''business associate'' to generally provide that a business associate includes a person who ''creates, receives, *maintains*, or transmits'' PHI on behalf of a covered entity.''[6]

Resolving an issue of long-standing concern to the research community, OCR noted that an external researcher hired or contracted by a covered entity to perform research is not a business associate because a business associate relationship exists only in cases where the person is assisting in the performance of a covered entity function regulated under HIPAA.[7] Similarly, an institutional review board is not a business associate of a covered entity based upon its research review, approval, and continuing oversight functions.[8]

New Obligations of Business Associates

Prior to the HITECH Act, business associates were not directly regulated under HIPAA (unless the business associate also was a covered entity), and a violation of a business associate agreement merely subjected the business associate to potential contractual damages. The HITECH Act, and now the Final Rule, extends new privacy and security obligations to business associates, who may now be directly subject to criminal and civil sanctions for violations of HIPAA.

The HIPAA Security Rule

The Final Rule requires business associates to comply with the Security Rule's administrative, technical and physical safeguard requirements and to implement security policies and procedures in the same manner as a covered entity.[9] Although OCR expresses a view that most business associates should already have in place security practices that either comply with the Security Rule or require only ''modest improvements'' to come into compliance,[10] that statement appears disingenuous—implementing a Security Rule compliance program can be costly.

The HIPAA Privacy Rule

In contrast to the approach taken with the Security Rule described above, the Final Rule does not impose

[2] 78 Fed. Reg. at 5688 (to be codified at 45 C.F.R. § 160.103 (definition of ''Business associate'')).

[3] 78 Fed. Reg. at 5573.

[4] 78 Fed. Reg. at 5689 (to be codified at 45 C.F.R. § 160.103 (definition of ''Subcontractor'')).

[5] 78 Fed. Reg. at 5572.

[6] 78 Fed. Reg. at 5688 (to be codified at 45 C.F.R. § 160.103 (definition of ''Business associate'')).

[7] 78 Fed. Reg. at 5575.

[8] *Id.*

[9] 78 Fed. Reg. at 5692 (to be codified at 45 C.F.R. § 164.104(b)).

[10] 78 Fed. Reg. at 5589.

  HLR ISSN 1064-2137

all of a covered entity's Privacy Rule obligations upon business associates. Instead, business associates may be subject to HIPAA penalties if they violate the required terms of their business associate agreements.

Under the Final Rule, business associates may be directly liable under the Privacy Rule for:

- uses and disclosures of PHI in violation of a business associate agreement or the Privacy Rule;
- failing to disclose PHI to the secretary of HHS (Secretary) to investigate the business associate's compliance with the Privacy Rule;
- failing to disclose PHI to comply with an individual's request for an electronic copy of PHI; and
- failing to make reasonable efforts to limit uses and disclosures of PHI, and PHI requested from a covered entity, to the minimum necessary to accomplish the intended purpose.[11]

Subcontractor Business Associate Agreements

Prior to the HITECH Act, business associates were required to ''ensure'' that a subcontractor ''agree'' to the same privacy and security obligations that apply to the business associate with respect to PHI.[12] This provision often led business associates to enter into written agreements with subcontractors, but a written agreement was not expressly required. The Final Rule requires a business associate to enter into a written agreement with a subcontractor in order to obtain satisfactory assurances that the subcontractor will comply with applicable provisions of the Privacy and Security Rules.[13]

OCR notes that the obligation to enter into a business associate agreement with a subcontractor rests solely with the business associate, and not the covered entity.[14] A covered entity is not required to enter into an agreement with a subcontractor of its business associate. The form of a subcontractor business associate agreement would be identical to the ''upstream'' business associate agreement and would contain all of the same required provisions. Each agreement in the business associate chain must be at least as stringent as the agreement above it in the chain with respect to permissible uses and disclosures. For example, if the agreement between a covered entity and its business associate does not permit de-identification of PHI, then no subcontractor business associate agreement in the chain may permit de-identification.[15]

If a business associate becomes aware of a pattern or practice of activity of a subcontractor that would constitute a material breach or violation of the subcontractor business associate contract, then the business associate must take reasonable steps to cure the breach or to terminate the contract, if feasible.[16] Prior to the HITECH Act, a similar obligation had been imposed upon covered entities that became aware of violations or material breaches of a business associate contract by a business associate.[17]

The Final Rule eliminates a requirement that covered entities report to the Secretary when, despite a material breach or violation by the business associate, termination of the business associate contract is not feasible. Given that under the HITECH Act business associates are now directly liable for HIPAA violations, and both covered entities and business associates are required to report certain breaches of unsecured PHI to the Secretary, HHS deemed the requirement unnecessary.[18]

Amendment of Business Associate Agreements

The Final Rule requires that the following new provisions be added to business associate contracts:

- The so-called ''safeguards'' provision should be replaced with a provision requiring that business associates ''use appropriate safeguards and comply, where applicable, with [the Security Rule], with respect to electronic PHI, to prevent use or disclosure of the information other than as provided for by its contract.''
- Business associates must report to the covered entity any breach of unsecured PHI, as required by the Breach Notification Rule. This requirement would be in addition to existing requirements that business associates report unauthorized uses and disclosures of PHI under the Privacy Rule and security incidents under the Security Rule.
- Business associates must enter into written agreements with subcontractors that create or receive PHI on behalf of the business associate imposing the same restrictions that apply to the business associate with respect to the PHI.
- Business associates must comply with the requirements of the Privacy Rule to the extent that the business associate is to carry out a covered entity's obligation under the Privacy Rule.[19] For example, if a business associate is providing an individual with access to PHI, that access must be provided in accordance with Privacy Rule requirements. However, OCR clarifies that when a business associate is performing such a delegated Privacy Rule compliance obligation, the covered entity remains directly liable under HIPAA for any violation, and the business associate is only contractually liable to the covered entity.[20]

On Jan. 25, OCR posted new template business associate provisions on its website that address Final Rule requirements.[21]

---

[11] 78 Fed. Reg. at 5590; 78 Fed. Reg. at 5696 (to be codified at 45 C.F.R. § 164.502(a)(3)).

[12] 45 C.F.R. § 164.504(e)(2)(ii)(D).

[13] 78 Fed. Reg. at 5697 (to be codified at 45 C.F.R. § 164.502(e)(1)(ii)).

[14] 78 Fed. Reg. at 5573, 5697 (to be codified at 45 C.F.R. § 164.504(e)(1)(i)).

[15] 78 Fed. Reg. at 5601.

[16] 78 Fed. Reg. at 5697 (to be codified at 45 C.F.R. § 164.504(e)(1)(iii)).

[17] 45 C.F.R. § 164.504(e)(1)(ii).

[18] 78 Fed. Reg. at 5600.

[19] 78 Fed. Reg. at 5697 (to be codified at 45 C.F.R. § 164.504(e)(2)).

[20] 78 Fed. Reg. at 5600.

[21] U.S. Dep't of Health & Human Servs., *Sample Business Associate Agreement Provisions* (Jan. 25, 2012) (*see related report in this issue*), http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

Compliance Date for Business Associate Contract Amendments

The Final Rule creates a transition period for amending business associate contracts in order to ''prevent rushed and hasty changes'' to thousands of ongoing business associate agreements.[22] The Final Rule provides that (i) if a business associate contract that is compliant with pre-HITECH Act business associate contracting requirements is entered into prior to the publication date of the Final Rule (Jan. 25) and (ii) the contract is not renewed or modified between March 26–Sept. 23, 2013, then the contract will be deemed to be compliant until the earlier of (i) the date the contract is renewed or modified on or after Sept. 23, 2013, or (ii) Sept. 23, 2014.[23]

In short, covered entities have a transition period for amending business associate contracts that may extend for as long as one year and eight months after the publication of the Final Rule. Existing business associate contracts that are renewed or modified by March 26 would qualify for the transition period. If a business associate contract is subject to automatic or ''evergreen'' renewal, such a renewal would not end the period of deemed compliance.[24] OCR notes that an agreement that requires ''compliance with all applicable laws'' is not sufficient to meet the Final Rule's requirements—HITECH Act-specific contract provisions are necessary.[25]

Covered entities and businesses associates will need to reevaluate their business associate contracting strategies in light of the Final Rule, weighing whether they wish to take full advantage of the contracting transition period, or whether business and liability considerations favor sooner amendment.

Penalties

The Final Rule amends the HIPAA regulations to provide that business associates that violate the Privacy or Security Rules may be directly liable for civil money penalties.[26] Conforming references to ''business associates'' are added throughout the civil money penalty provisions. In addition, a business associate is liable, in accordance with the federal common law of agency, for violations based upon the acts or omissions of agents, including workforce members and subcontractors, acting within the scope of the agency.[27]

Liability of Covered Entities for Violations by Business Associates

The Enforcement Rule currently provides an exception for covered entity liability for the acts of an agent when (i) the agent is a business associate, (ii) the relevant contract requirements have been met, (iii) the covered entity did not know of a pattern or practice of the business associate in violation of the contract, and (iv) the covered entity did not fail to act as required by the Privacy or Security Rule with respect to the violations. The Final Rule eliminates this exception, making covered entities directly liable for the actions of business associates who are agents within the meaning of federal common law.[28] For business associates who are ''independent contractors'' rather than ''agents,'' the ''pattern or practice'' rule described above still would apply.

The determination of whether a business associate is an agent will be fact-specific, but OCR states that the ''essential factor'' in determining whether an agency relationship exists is the right or authority of the covered entity to control the conduct of the business associate in performing its services.[29] Significantly, OCR notes that the ability of a covered entity to give interim instructions or directions is the type of control that suggests an agency relationship. If a business associate is performing its duties strictly in accordance with the terms of its agreement with the covered entity, and the only means for the covered entity to exercise further controls is through a contract amendment, then the business associate is probably not acting as an agent.[30] It is important to note HHS's comment that a covered entity's liability for the violations of an agent business associate is not contingent upon the execution of a business associate contract.

Breach Notification Rule

The HITECH Act set forth new standards for breach notification in the health care industry, requiring covered entities to provide notification to affected individuals, the Secretary and, in some instances, to the media, following the discovery of a breach of unsecured PHI. The HITECH Act also required business associates to notify covered entities of the breach, when the breach of unsecured PHI occurred at or by the business associate. The Breach Notification Interim Final Rule (Interim Final Rule) introduced a ''harm standard,'' meaning that only those breaches that posed a significant risk of financial, reputational or other risk of harm to the individual would trigger the notification requirement.[31] Under the Breach Notification Rule, covered entities and business associates were required to perform a risk assessment to determine if there was a significant risk of harm to the individual as a result of the breach. When OCR withdrew the Interim Final Rule from review by the Office of Management and Budget in July 2010, it was widely speculated that the harm standard was being reconsidered, and that proved to be the case.

In the Final Rule, OCR significantly modifies the definition of a ''breach,'' removing the ''harm standard,'' and thereby making it seemingly more likely that a breach will trigger the notification requirement. In the commentary to the Final Rule, OCR notes that its new approach to breach notification is a response to commenters who requested a ''more objective'' standard for breach notification, whereby risk assessments would focus on the risk that the PHI was compromised rather than the risk of harm to the individual.[32] OCR also

[22] 78 Fed. Reg. at 5602.
[23] 78 Fed. Reg. at 5702 (to be codified at 45 C.F.R. § 164.532).
[24] 78 Fed. Reg. at 5603.
[25] *Id.*
[26] 78 Fed. Reg. at 5691 (to be codified at 45 C.F.R. § 160.402(a)).
[27] 78 Fed. Reg. at 5691 (to be codified at 45 C.F.R. § 160.402(c)(2)).
[28] 78 Fed. Reg. at 5691 (to be codified at 45 C.F.R. § 160.402(c)(1)).
[29] 78 Fed. Reg. at 5581.
[30] *Id.*
[31] 74 Fed. Reg. 42740 (Aug. 24, 2009).
[32] 78 Fed. Reg. at 5641.

  HLR ISSN 1064-2137

notes in the commentary to the Final Rule that because ''every breach of unsecured protected health information must have an underlying impermissible use or disclosure under the Privacy Rule,'' OCR has ''the authority to impose a civil money penalty for the underlying Privacy Rule violation, even in cases where all required breach notifications were provided.''[33] This means that, even if a covered entity has appropriately notified affected individuals of a breach, OCR may choose to impose civil penalties based upon the underlying Privacy Rule violation that gave rise to the breach.

- *Definition of Breach*. A ''breach'' is generally defined as the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information.[34] The Final Rule amends the definition of breach to include an express presumption whereby an impermissible use or disclosure of PHI is considered to be a breach unless the covered entity or business associate is able to demonstrate that there is a ''low probability'' that the PHI has been compromised.[35] Under the Final Rule, the term ''compromised'' is no longer defined. OCR acknowledges that its former approach to breach notification may have been interpreted as ''setting a much higher threshold for breach notification'' than intended.[36] While OCR declines to adopt a ''bright line approach'' to breach notification, OCR notes that its former approach that focused on harm to the individual was ''too subjective'' and resulted in ''inconsistent interpretations and results.'' OCR believes that this new focus on the risk that PHI has been compromised will enable covered entities and business associates to ''interpret and apply the regulation in a uniform manner.''[37]
- *Risk Assessment*. The Final Rule identifies four factors that covered entities and business associates must consider when performing a risk assessment to determine whether there is a low probability that PHI has been compromised.
  - *First*, evaluate the nature and the extent of the PHI involved. This means that covered entities and business associates should consider the type of PHI involved, including the types of identifiers and the likelihood of re-identification.
  - *Second*, consider the individual who impermissibly used the PHI or to whom the impermissible disclosure was made.
  - *Third*, investigate whether the PHI was actually acquired or viewed or, if only the *opportunity* existed for the information to be acquired or viewed.
  - *Fourth*, consider the extent to which the risk to the PHI has been mitigated. For instance, covered entities and business associates may mitigate such risks by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed or will be destroyed, and can take into account the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised.[38]

Taking into account these factors, as well as additional factors as necessary, covered entities and business associates must then evaluate the overall probability that the PHI has been compromised by engaging in a good faith, thorough analysis of all of the factors in order to reach a conclusion. If such an evaluation fails to demonstrate that there is a low probability that the PHI has been compromised, breach notification is required. OCR suggests that covered entities and business associates examine their current policies to ensure that all required factors are considered when conducting a risk assessment. OCR notes that it plans to provide additional guidance to aid covered entities and business associates in performing risk assessments by highlighting certain ''frequently occurring scenarios.''[39]

- *Limited Data Sets*. Under the Final Rule, OCR removes the exception set forth in the Interim Final Rule for limited data sets that do not contain any dates of birth and ZIP codes.[40] Rather, covered entities and business associates are required to perform a risk assessment following the impermissible use or disclosure of any limited data set. OCR is therefore encouraging covered entities and business associates to encrypt limited data sets and other PHI in order to take advantage of the safe harbor provision of the Breach Notification Rule, reiterating that the impermissible use or disclosure of encrypted PHI would not trigger the requirement for a breach notification.[41]
- *HHS Notice*. The Final Rule makes one modification to the requirement that covered entities notify HHS of any breach. Under the Final Rule, if fewer than 500 individuals are affected, the covered entity may maintain a log to be produced to HHS annually, which must now be submitted to HHS not later than 60 days after the end of the calendar year in which the breach was ''*discovered*,'' rather than when the breaches ''occurred.''[42] If the disclosure involves the PHI of more than 500 individuals, HHS must be notified ''without unreasonable delay but in no case later than 60 calendar days following discovery of a breach.''[43]
- *Notice to Individuals*. The Final Rule retains the requirements for individual notice set forth in the Breach Notification Rule without modification, noting that the covered entity ''ultimately maintains the obligation to notify affected individuals of the breach.''[44] OCR does clarify certain issues relating to individual notification, noting, for instance, that notice is not considered to be provided when a written notice is returned as undeliverable. When more than 10 notifications are returned as undeliverable, reasonable time may be taken to search for correct, current addresses, but alternate notice must be

[33] 78 Fed. Reg. at 5658.
[34] 45 C.F.R. § 164.402.
[35] 78 Fed. Reg. at 5641 (to be codified at 45 C.F.R. § 164.402).
[36] 78 Fed. Reg. at 5641.
[37] *Id*.
[38] 78 Fed. Reg. at 5642–43.
[39] 78 Fed. Reg. at 5643.
[40] 78 Fed. Reg. at 5644.
[41] *Id*.
[42] 78 Fed. Reg. at 5654 (to be codified at 45 C.F.R. § 164.408(c)).
[43] 78 Fed. Reg. at 5653 (to be codified at 45 C.F.R. § 164.408(b)).
[44] 78 Fed. Reg. at 5650 (to be codified at 45 C.F.R. § 164.404(d)).

provided ''as soon as reasonably possible'' and no later than the original 60-day deadline.[45]

- *Media Notice*. OCR notes that covered entities are not obligated to incur the cost of any media broadcast regarding the breach at issue.[46] OCR also notes that media outlets are not obligated to publicize every breach notice they receive. OCR emphasizes that for purposes of providing media notice, it would not be sufficient for a covered entity to post a press release regarding a breach on its home page.[47]

The Privacy Rule

Marketing

OCR has had long-standing concerns with situations in which third parties subsidize communications between covered entities and patients and has steadily increased regulation of this area under the Privacy Rule and the HITECH Act. The Final Rule significantly modifies the approach to marketing set forth in the Proposed Rule, requiring covered entities to obtain authorization from individuals for *all* treatment and health care operations communications where the covered entity receives financial remuneration for making the communications from a third party whose product or service is being marketed.[48] OCR acknowledges the difficulty that covered entities may face in determining whether a communication is for treatment or health care operations purposes and, therefore, believes that the best policy is to require authorizations for all subsidized communications that market a health-related product or service.[49]

OCR has also decided that individuals will be sufficiently notified of such communications through the authorization process and has decided not to require a covered entity to include in its notice of privacy practices the proposed notice and opt-out requirements for treatment communications involving remuneration from a third party, as set forth in the Proposed Rule.[50] Likewise, OCR has decided not to retain the current requirement that covered entities include a statement in their notice of privacy practices informing individuals that they may be contacted to provide appointment reminders or information about treatment alternatives or other health-related benefits and services.[51]

OCR also clarifies that an authorization is required when a business associate (including a subcontractor), rather than the covered entity, receives financial remuneration from a third party in exchange for making a communication about a product or service.[52]

The Final Rule adopts the Proposed Rule's definition of ''financial remuneration'' for purposes of the marketing rules as ''direct or indirect payment from or on behalf of a third party whose product or service is being described.''[53] Direct or indirect payment does not include any payment for treatment of an individual. In the Final Rule, OCR clarifies that, for purposes of the marketing rules, ''direct payment'' means ''financial remuneration that flows from the third party whose product or service is being described directly to the covered entity,'' whereas ''indirect payment'' includes ''financial remuneration that flows from an entity on behalf of the third party whose product or service is being described to a covered entity.''[54] OCR confirms that the term ''financial remuneration'' is limited to payments made in exchange for making a communication about a product or service, and does not include nonfinancial benefits, such as in-kind benefits, received by a covered entity in exchange for making such communications.[55]

The Final Rule adopts the exceptions to the authorization requirement for marketing communications set forth in the Proposed Rule and, therefore, no authorization is required where the communication is (i) in the form of a face-to-face communication made by a covered entity to an individual; or (ii) a promotional gift of nominal value provided by the covered entity.[56]

The Final Rule also largely adopts the exceptions to marketing communications set forth in the Proposed Rule, and thus a communication is not considered a marketing communication if it is made:

- to provide refill reminders or communicate about a drug or biologic currently prescribed to the individual, provided any remuneration received for making the communication is reasonably related to the cost of making the communication;
- for the following treatment and health care purposes, except where the covered entity receives financial remuneration in exchange for making the communication;
  - for treatment of an individual by a health care provider (including for case management or care coordination or to recommend alternative treatments, therapies, health care providers, or settings of care to the individual);
  - to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication; or
  - for case management or care coordination, contacting individuals with information about treatment alternatives, and related functions, to the extent these activities do not fall within the definition of treatment.[57]

Fund-Raising

The HITECH Act required HHS to issue a rule that requires all written fund-raising communications from a covered entity to provide the recipient with an opportunity to opt out of any future fund-raising communications. Implementing this requirement, the Final Rule provides:

[45] 78 Fed. Reg. at 5652.
[46] 78 Fed. Reg. at 5653.
[47] *Id*.
[48] 78 Fed. Reg. at 5595.
[49] *Id*.
[50] 78 Fed. Reg. at 5596 (to be codified at 45 C.F.R. § 164.514(f)(2)).
[51] 78 Fed. Reg. at 5595.
[52] 78 Fed. Reg. at 5595–96.
[53] 78 Fed. Reg. at 5595.
[54] *Id*.
[55] 78 Fed. Reg. at 5596.
[56] 78 Fed. Reg. at 5699 (to be codified at 45 C.F.R. § 164.508(3)(i)(A)–(B)).
[57] 78 Fed. Reg. at 5696 (to be codified at 45 C.F.R. § 164.501 (definition of ''Marketing'')).

  HLR ISSN 1064-2137

- each fund-raising communication must include a clear and conspicuous opportunity for the individual to elect not to receive further fund-raising communications (once again, the individual should not incur an undue burden or more than a nominal cost, and HHS prefers a toll-free phone number, local phone number, email address, preprinted and prepaid postcard, or similar method);
- treatment or payment cannot be conditioned on an individual's choice to receive fund-raising communications;
- fund-raising communications may not be sent to someone who has opted out of such communications;
- a covered entity may provide an individual who has opted out of fund-raising communications with a method to opt back in; and
- a covered entity must include a statement in its notice of privacy practices that the entity may use and disclose PHI for fund-raising but that individuals have the right to opt out of receiving such communications.[58]

The Privacy Rule had required that a covered entity make reasonable efforts to ensure that individuals who opt out do not receive further communications. In keeping with the HITECH Act's provisions, the Final Rule toughens that standard by simply making any further fund-raising communications with a person who has opted out a violation of the Privacy Rule. This provision is intended to effectuate the intent of the HITECH Act's requirement that a fund-raising opt out operate like a revocation of authorization.[59] Despite the HITECH Act's reference to written communications, the Final Rule applies this rule to fund-raising communications made in any form, including over the phone.

After soliciting comments on the subject, OCR decided to leave the scope of the opt out to the discretion of the covered entity in the Final Rule, meaning that a covered entity may offer an opt-out with respect to all future fund-raising communications or only a specific campaign.[60] Similarly, covered entities have discretion in determining how to permit an individual to opt back in. Once an individual has opted out of fund-raising communications, that opt-out cannot automatically lapse, and an active opt-in is required.[61]

The Final Rule also clarifies and expands the categories of information that a covered entity may utilize for fund-raising purposes to include the following: (i) demographic information, including name, address, other contact information, age, gender, and date of birth; (ii) dates of health care provided to an individual; (iii) department of service information; (iv) treating physician; (v) outcome information; and (vi) health insurance status.[62]

Sale of PHI

The HITECH Act generally prohibits a covered entity or business associate from receiving direct or indirect remuneration in exchange for the disclosure of PHI unless the covered entity or business associate has obtained an authorization from the individual that states whether the PHI can be further exchanged for remuneration by the entity receiving the information.

The Final Rule largely adopts the exceptions set forth in the Proposed Rule, providing that the prohibition does not apply if the purpose of the exchange is:

- public health activities;
- research, so long as the payment is a ''reasonable, cost-based fee'' reflecting the costs of preparing and transmitting the PHI for such purpose;
- treatment and payment purposes;
- the sale, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that, following such activity, will become a covered entity, and due diligence related to such activity;
- disclosures that are otherwise required by law;
- remuneration that is provided by a covered entity to a business associate for activities involving the exchange of PHI that the business associate undertakes on behalf of, and at the specific request of, the covered entity pursuant to a business associate agreement (note that this also applies to remuneration that is provided by a business associate to a subcontractor, where applicable);
- remuneration received by a covered entity or a business associate, provided that it is a ''reasonable, cost-based fee'' to cover the cost to prepare and transmit records on behalf of a covered entity; or
- to provide an individual with a copy of the individual's PHI or an accounting of disclosures pursuant to a request by the individual.[63]

The Final Rule adopts the HITECH Act's prohibition on the sale of PHI, but clarifies and/or makes certain changes to the following provisions set forth in the Proposed Rule:

- In response to commenters, OCR has included in the Final Rule a definition of ''sale of protected health information'' that includes disclosures of PHI by both a covered entity or a business associate, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.[64]
- For purposes of the sale of PHI, the term ''remuneration'' includes both financial as well as nonfinancial benefits. For example, OCR states that if a covered entity is offered computers in exchange for disclosing PHI, that arrangement may or may not constitute a sale of PHI, depending upon the circumstances. If the computers were only used to prepare and transmit PHI to the person collecting it, and returned after the disclosure was completed, that would not constitute a sale of PHI. If, however, the covered entity used the computers for other purposes or kept

[58] 78 Fed. Reg. at 5700 (to be codified at 45 C.F.R. § 164.514(f)(2)).
[59] 78 Fed. Reg. at 5618.
[60] 78 Fed. Reg. at 5621.
[61] *Id.*
[62] 78 Fed. Reg. at 5700 (to be codified at 45 C.F.R. § 164.514(f)(1)).
[63] 78 Fed. Reg. at 5697 (to be codified at 45 C.F.R. § 164.502(a)(5)(ii)(B)(2)).
[64] 78 Fed. Reg. at 5697 (to be codified at 45 C.F.R. § 164.502(a)(5)(ii)(B)(1)).

the computers even after the disclosures had been made, then the covered entity would have received in-kind remuneration in exchange for disclosing PHI.[65]

- A ''sale'' of PHI includes transactions that result in access, license or lease agreements, and is not restricted to transactions transferring ownership of PHI.[66]
- Grants, contracts or other arrangements entered into by a covered entity to perform programs or activities, such as a research study, are not considered a sale of PHI; and[67]
- Exchange of PHI through a health information exchange (HIE) that is paid for through fees assessed on HIE participants is not a sale of PHI.[68]

While HHS has declined to exempt limited data sets from the remuneration prohibition, since unlike de-identified data, they still constitute PHI, limited data sets will be exempt from the authorization requirements to the extent the only remuneration received in exchange for the data is a ''reasonable, cost-based fee to prepare and transmit the data or a fee otherwise expressly permitted by other law.''[69]

Requests for Restrictions on Disclosures of PHI

The Privacy Rule currently provides individuals with a right to request a restriction on a covered entity's use or disclosure of PHI for treatment, payment or health care operations purposes, but covered entities are not required to grant such requests. The HITECH Act created an exception to this rule, providing that a covered entity must comply with a requested restriction if the disclosure is (i) to a health plan for purposes of carrying out payment or health care operations (and not for treatment), (ii) not otherwise required by law, and (iii) the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out-of-pocket in full.

The Final Rule implements this new HITECH Act requirement,[70] and OCR offers clarifying comments. Health care providers are not required to create separate medical records or segregate PHI subject to a restriction, but they will need to use some method to flag or notate the records to ensure that they are not inadvertently sent to or accessed by a health plan.[71] OCR acknowledges that it is unworkable, given the current state of technology, to require a provider to notify downstream providers that an individual has requested a restriction, so patients would be responsible for requesting that other providers apply a restriction.[72]

A Medicare beneficiary may request a restriction on the disclosure of PHI with respect to a Medicare-covered service by refusing to authorize the submission of a bill to Medicare for the service and paying out-of-pocket.[73] When a service is bundled with other services, providers will be expected to advise the patient on the options for unbundling the service and paying for it out-of-pocket or paying for the entire bundle of items and services.[74] If a health maintenance organization (HMO) provider is prohibited by law from accepting payment from the individual above cost-sharing amounts, then the provider may advise the individual that he or she will have to use an out-of-network provider in order to pay out-of-pocket for the service and restrict disclosure of PHI to the HMO.[75]

Access to Electronic PHI

The Privacy Rule gives individuals the right to obtain copies of their PHI from a covered entity, to the extent the information is maintained in a designated record set. The HITECH Act expanded those access rights with respect to PHI maintained in an EHR, allowing the individual to obtain a copy of the information in an electronic format and direct the covered entity to transmit the copy directly to a person or entity designated by the individual, so long as the choice is clear, conspicuous and specific.

In the commentary to the Proposed Rule, OCR noted that granting these access rights with respect to EHRs, but not other electronic PHI maintained in designated record sets, would result in a complex set of disparate requirements for access to electronic PHI.[76] Therefore, in the Proposed Rule and now the Final Rule, OCR extends the HITECH Act's access right to all PHI maintained electronically by a covered entity. Covered entities would be required to provide the information in the electronic form and format requested by the individual, if it is readily producible or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.[77] Acceptable formats may include Microsoft Word, Excel, text, HTML, or text-based PDF.

In a change introduced in the Final Rule, OCR eliminated the Privacy Rule provision that permitted 60 days for providing access when PHI is not maintained or accessible to the covered entity on-site. OCR retained the provision that permits a covered entity a one-time extension of 30 days to respond to the individual's request for access, noting its view that the 30-day time frame is appropriate given the increasing ability to provide almost instantaneous access to electronic PHI.[78]

The Final Rule allows a covered entity to charge for electronic media on which electronic records are provided, unless the individual supplies the media or requests transmission by email.[79] The HITECH Act provided that any fee charged by the covered entity for providing access to EHR data may not be greater than its labor costs in responding to the request. In response to requested comments, OCR clarifies that labor costs included in a reasonable cost-based fee could include

[65] 78 Fed. Reg. at 5607.
[66] 78 Fed. Reg. at 5606.
[67] *Id.*
[68] *Id.*
[69] 78 Fed. Reg. at 5609.
[70] 78 Fed. Reg. at 5701 (to be codified at 45 C.F.R. § 164.522(a)(1)(vi)).
[71] 78 Fed. Reg. at 5628.
[72] 78 Fed. Reg. at 5629.
[73] 78 Fed. Reg. at 5628.
[74] 78 Fed. Reg. at 5629.
[75] *Id.*
[76] 78 Fed. Reg. at 5631.
[77] 78 Fed. Reg. at 5702 (to be codified at 45 C.F.R. § 164.524(c)(2)(i)).
[78] 78 Fed. Reg. at 5701–02 (to be codified at 45 C.F.R. § 164.524(b)(2)(ii)).
[79] 78 Fed. Reg. at 5702 (to be codified at 45 C.F.R. § 164.524(c)(4)(ii)).

  HLR ISSN 1064-2137

skilled technical staff time spent creating and copying the electronic file.[80]

The Final Rule also would grant the individual a new right to direct the covered entity in writing to send a paper copy of PHI to a third party; the HITECH Act only had extended that right to electronic PHI in an EHR.[81]

Notice of Privacy Practices

The Final Rule mandates that the following changes be made to a covered entity's notice of privacy practices, largely tracking the Proposed Rule:

- While the notice need not include a list of all situations that require authorization, the notice must describe the need for an authorization for most uses and disclosures of psychotherapy notes (where appropriate), uses and disclosures of PHI for marketing purposes, and disclosures that constitute the sale of PHI.
- Since the Final Rule now considers all subsidized treatment communications to be marketing communications, the notice need not contain a statement about such communications or the ability of an individual to opt out.
- If, however, the covered entity intends to send fund-raising solicitations, the notice of privacy practices must notify the individual of the right to opt out (in contrast to the current Privacy Rule requirement to simply include notice of the opt-out right in the solicitation).
- The notice must inform the individual that the covered entity may not refuse a request to withhold information from a health plan where the individual pays out-of-pocket in full for the service.
- The notice must include a statement of the right of affected individuals to be notified of a breach of unsecured PHI.[82]

Because OCR views these modifications as material, covered entities will be required to promptly revise and distribute amended notices.[83] Under the Final Rule, a health plan that currently posts its notice of privacy practices on its website must (i) prominently post the change or its revised notice on its website by the effective date of the material change to the notice (*i.e.*, the compliance date of the Final Rule), and (ii) provide the revised notice or information about the material change and how to obtain the revised notice in its next annual mailing to plan members.[84] A health plan that does not maintain a customer service website must provide the revised notice, or information about the material change and how to obtain the revised notice, to plan members within 60 days of the material revision to the notice.[85] The Final Rule does not modify health care providers' current obligations to make revised notices available.[86]

The Minimum Necessary Rule

The Privacy Rule requires covered entities to limit uses and disclosures of, and requests for, PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. The HITECH Act provides that a covered entity shall be treated as being in compliance with the minimum necessary rule only if the covered entity limits the PHI used or disclosed, to the extent practicable, to the limited data set or, if needed by the covered entity, to the minimum necessary.

The Final Rule adopts the Proposed Rule's provision applying the minimum necessary standard directly to business associates (including subcontractors). The Final Rule further clarifies that requests directed to another business associate must also be limited to the minimum necessary.[87] OCR intends to issue further guidance addressing business associates' application of the minimum necessary standard.[88]

Decedents

The Privacy Rule has required that covered entities protect the privacy of a decedent's PHI to the same extent as the PHI of a living individual. Therefore, when an authorization is required for disclosure of PHI, a covered entity may disclose a decedent's PHI only after obtaining a written authorization from the decedent's personal representative, which can have the effect of limiting disclosures to family and friends. OCR noted concerns have been raised regarding the difficulty of locating a personal representative to authorize disclosure of PHI, particularly after the decedent's estate has closed.[89]

The Final Rule:

- allows a covered entity to disclose PHI to a family member, other relative, or a close personal friend of the decedent, or any other person identified by the individual, unless doing so is inconsistent with a prior expressed preference of the decedent;[90] and
- removes all privacy protections for records of persons deceased for more than 50 years.[91]

OCR emphasizes that the 50-year period of protection does not constitute a record retention requirement and covered entities may destroy decedent medical records as permitted by applicable law. In addition, the 50-year protection period does not override other laws that may provide greater protections for information of decedents relating to sensitive categories of information, such as HIV/AIDS, substance abuse, mental health information or psychotherapy notes.[92]

Research Authorizations

The Privacy Rule generally prohibits covered entities from conditioning treatment on the provision of an authorization. However, a covered entity is permitted to

---

[80] 78 Fed. Reg. at 5636.

[81] 78 Fed. Reg. at 5702 (to be codified at 45 C.F.R. § 164.524(c)(3)(ii)).

[82] 78 Fed. Reg. at 5701 (to be codified at 45 C.F.R. § 164.520(b)(1)(ii)(E)).

[83] 78 Fed. Reg. at 5625.

[84] 78 Fed. Reg. at 5701 (to be codified at 45 C.F.R. § 164.520(c)(1)(v)(A)).

[85] 78 Fed. Reg. at 5701 (to be codified at 45 C.F.R. § 164.520(c)(1)(v)(B)).

[86] 78 Fed. Reg. at 5701 (45 C.F.R. § 164.520(c)(2)(iii)–(iv))

[87] 78 Fed. Reg. at 5697 (to be codified at 45 C.F.R. § 164.502(b)).

[88] 78 Fed. Reg. at 5599.

[89] 78. Fed. Reg. at 5613.

[90] 78 Fed. Reg. at 5699 (to be codified at 45 C.F.R. § 164.510(b)(5)).

[91] 78 Fed. Reg. at 5697 (to be codified at 45 C.F.R. § 164.502(f)).

[92] 78 Fed. Reg. at 5614.

condition the provision of research-related treatment on obtaining the individual's authorization, such as for a clinical trial (a ''conditioned authorization''). The Privacy Rule also generally prohibits compound authorizations in which two authorizations are combined in one document.

OCR heeded concerns from commenters that recruitment for clinical research trials has been hampered by the numerous forms that must be signed to participate in clinical trials and related activities, such as tissue banking and specimen collection for a central repository.[93] To address this issue, the Final Rule permits a covered entity to combine conditioned and unconditioned authorizations for research, provided that the authorization differentiates between the conditioned and unconditioned research components and clearly allows the individual to opt in to the unconditioned research activities.[94]

Although it does not reflect a change to regulatory provisions, OCR modified its prior interpretation that research authorizations must be study-specific. In order to satisfy the requirement that an authorization describe the purpose of each requested use or disclosure, an authorization for future research purposes must adequately describe the purposes so that the individual would reasonably expect that his or her PHI could be used for such future research. OCR noted that this approach harmonizes HIPAA with practices under the Common Rule regarding informed consent for future research.[95]

Student Immunization Records

The Final Rule permits covered entities to disclose proof of immunization to schools in states that have school entry or similar laws.[96] By providing this ''permissive'' disclosure in an effort to ''promote public health by reducing the burden associated with providing schools with student immunization records,'' OCR responds to concerns that the Privacy Rule has made it more difficult for parents to provide, and for schools to obtain, necessary immunization documentation for students.[97] Most states have ''school entry laws'' that prohibit a child from attending school unless the school has proof that the child has been appropriately immunized.

In response to these concerns, the Final Rule amends a covered entity's permitted uses and disclosures for public health activities to permit covered entities to disclose proof of immunization to schools in states that have school entry or similar laws. While written authorization will no longer be required for such disclosures, the covered entity will still be required to obtain an agreement, which may be oral, from a parent, guardian or other person acting for the individual, or directly from the individual if he or she is an emancipated minor.[98] The Final Rule confirms that such agreement must be documented in writing, although this documentation does not require signature by the appropriate individual.[99]

Genetic Information

The Final Rule, in accordance with GINA and the Proposed Rule, prohibits the use or disclosure of PHI that is genetic information for underwriting purposes by health plans.[100] OCR used its regulatory authority to apply this prohibition to all health plans regulated under HIPAA, with the exception of long-term care insurers, which is broader than the scope provided for under GINA. The Final Rule's definition of ''underwriting'' includes an exception for determinations of medical appropriateness. For example, if an individual is seeking a benefit under a plan and the plan needs genetic information to determine the medical appropriateness of providing the benefit, such as coverage for mammograms under age 40 based upon an increased risk for breast cancer, the plan may use or disclose the minimum necessary amount of genetic information for that determination.[101] A health plan that intends to use or disclose PHI for underwriting purposes must add a statement to its notice of privacy practices providing that it will not use or disclose genetic information for such purposes. The Final Rule's restrictions regarding genetic information do not apply to health care providers.

Enforcement

The HITECH Act introduced a variety of new measures aimed at strengthening HIPAA enforcement efforts, including increased civil penalties. The Enforcement Rule issued by OCR in October 2009 sought to implement the HITECH Act's changes. The Final Rule adopts additional modifications to the Enforcement Rule and clarifies certain key terms introduced by the Proposed Rule.

The Final Rule adopts the Proposed Rule's proposal to include references to business associates throughout the Enforcement Rule, thereby implementing the HITECH Act's provisions imposing direct liability on business associates for violations of the HITECH Act and the HIPAA Privacy and Security Rules.[102]

The Enforcement Rule currently provides that OCR *may* investigate privacy complaints or conduct compliance reviews. In accordance with the HITECH Act, the Final Rule adopts the provisions in the Proposed Rule to indicate that OCR *will* investigate complaints or conduct compliance reviews when a review of the facts indicates a potential violation due to willful neglect.[103] The Final Rule also adopts the proposed requirement for OCR to conduct a compliance review when a preliminary review of the facts indicates a possible violation due to willful neglect, meaning that OCR may initiate a compliance review even in the absence of a complaint when it becomes aware of facts indicating willful

[93] 78 Fed. Reg. at 5609.
[94] 78 Fed. Reg. at 5699 (to be codified at 45 C.F.R. § 164.508(b)(3)(i) and (iii)).
[95] 78 Fed. Reg. at 5612.
[96] 78 Fed. Reg. at 5700 (to be codified at 45 C.F.R. § 164.512(b)(1)).
[97] 78 Fed. Reg. at 5618.
[98] 78 Fed. Reg. at 5700 (to be codified at 45 C.F.R. § 164.512(b)(1)(vi)).
[99] 78 Fed. Reg. at 5617.
[100] 78 Fed. Reg. at 5696 (to be codified at 45 C.F.R. § 164.502(a)(5)).
[101] 78 Fed. Reg. at 5665.
[102] 78 Fed. Reg. at 5577.
[103] 78 Fed. Reg. at 5690 (to be codified at 45 C.F.R. § 160.306(c)(1)).

  HLR ISSN 1064-2137

neglect.[104] OCR is no longer required to resolve cases of noncompliance due to willful neglect by informal means, such as demonstrated compliance or a corrective action plan.[105] OCR retains the ability to resolve cases not involving willful neglect through informal means.

The Final Rule confirms that OCR may disclose PHI if permitted under the federal Privacy Act.[106] These disclosures are necessary to permit the Secretary to cooperate with other law enforcement agencies, such as state attorneys general pursuing HIPAA actions on behalf of state residents or the Federal Trade Commission pursuing remedies under other consumer protection authorities.[107]

The HITECH Act's tiered penalty structure is based upon the following degrees of culpability: (i) violations of which the person did not know (and by exercising reasonable due diligence would not have known), (ii) violations due to reasonable cause and not willful neglect, and (iii) violations due to willful neglect. The Final Rule adopts the proposed modified definition of reasonable cause in order to clarify the demarcations between the categories of culpability.[108]

Under the Final Rule, ''reasonable cause'' is defined to mean: ''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.''[109] This revised definition adds the ''knowledge,'' ''reasonable diligence'' and ''willful neglect'' standards.

For consistency with the HITECH Act's tiered penalty structure, the Final Rule modifies the Enforcement Rule to explicitly state that OCR must consider ''the nature and extent of the violation'' and ''the nature and extent of the harm resulting from the violation'' in determining a civil money penalty amount. The Final Rule also includes the proposed reference to reputational harm as a cognizable form of harm to be considered in penalty determinations. OCR notes that its determination of whether reputational harm has occurred will be a ''fact-specific inquiry,'' and will not arise solely from the unlawful disclosure of particularly sensitive PHI, but rather will be based on a consideration of facts such as whether the unlawful disclosure resulted in ''adverse effects on employment, standing in the community, or personal relationships.''[110]

---

[104] 78 Fed. Reg. at 5690 (to be codified at 45 C.F.R. § 160.308(a)).

[105] 78 Fed. Reg. at 5690 (to be codified at 45 C.F.R. § 160.312(a)(1)).

[106] 78 Fed. Reg. at 5690 (to be codified at 45 C.F.R. § 160.310(c)(3)).

[107] 78 Fed. Reg. at 5579.

[108] 78 Fed. Reg. at 5580.

[109] 78 Fed. Reg. at 5691 (to be codified at 45 C.F.R. § 160.401 (definition of ''Reasonable cause'')).

[110] 78 Fed. Reg. at 5584–85, 5691 (to be codified at 45 C.F.R. § 160.408(a) and (b)).