ReedSmith

The business of relationships.SM

Reed Smith Client Alert

The HITECH Final Rule: The New Privacy/Security Rules of the Road Have Finally Arrived

Written by Brad M. Rostolsky, Nancy E. Bonifant, Salvatore G. Rotella, Jr., Elizabeth D. O'Brien, Jennifer Pike and Zachary A. Portin

February 19, 2013

ReedSmith

IF YOU HAVE QUESTIONS OR WOULD LIKE ADDITIONAL INFORMATION ON THE MATERIAL COVERED IN THIS ALERT, PLEASE CONTACT ONE OF THE AUTHORS:

Brad M. Rostolsky
Partner, Philadelphia
+1 215 851 8195
brostolsky@reedsmith.com

Nancy E. Bonifant
Associate, Washington, DC
+1 202 414 9353
nbonifant@reedsmith.com

Salvatore G. Rotella, Jr.
Partner, Philadelphia
+1 215 851 8123
srotella@reedsmith.com

Elizabeth D. O'Brien
Associate, Washington, DC
+1 202 414 9289
eobrien@reedsmith.com

Jennifer Pike
Associate, Washington, DC
+1 202 414 9218
jlpike@reedsmith.com

Zachary A. Portin
Associate, Philadelphia
+1 215 851 8185
zportin@reedsmith.com

...OR THE CHAIR OF THE LIFE SCIENCES HEALTH INDUSTRY GROUP

Carol C. Loepere
Partner, Washington, DC
+1 202 414 9216
cloepere@reedsmith.com

Table of Contents

Page

ReedSmith

ReedSmith

The HITECH Final Rule: The New Privacy/Security Rules of the Road Have Finally Arrived

Written by Brad M. Rostolsky, Nancy E. Bonifant, Salvatore G. Rotella, Jr., Elizabeth D. O'Brien, Jennifer Pike and Zachary A. Portin

Since the 2009 enactment of the Health Information Technology for Economic and Clinical Health Act (the "Act" or "HITECH Act"), compliance efforts associated with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") has remained clouded in uncertainty. On January 25, 2013, and after more than a three-year wait after the release of the July 14, 2010, proposed regulations (the "Proposed Rule"),[1] the Office for Civil Rights ("OCR") of the U.S. Department of Health and Human Services ("HHS") published the long-awaited HITECH final rule – 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 (the "Final Rule").[2]

When the HITECH Act was passed, it was clear that the true import of the Act would not be felt until HHS provided the industry with the associated updated and revised regulations. Though HHS gave us a glimpse of the Act's significance with the Proposed Rule, the Final Rule answers many of the questions (and prompts others) regarding how these changes to federal privacy and security regulations will impact the operations of covered entities and business associates.

The Final Rule serves as an omnibus rule, and in effect provides final regulations with regard to four distinct aspects of previously proposed rulemakings. The Final Rule implements final rulemaking with regard to the Proposed Rule, the 2009 (interim final) Breach Notification Rule, the 2009 (interim final) Enforcement Rule, and the 2009 Genetic Information Nondiscrimination Act ("GINA") proposed rule. As was expected, the Final Rule does not address the May 2011 proposed accounting and access report rule.

Key Compliance Dates

- General Compliance Date – Sept. 23, 2013
- Enforcement Rule Compliance Date – March 26, 2013
- BAA Grandfather Period – Through Sept. 22, 2014

The Final Rule, which is effective on March 26, 2013, generally allows covered entities and business associates 180 days after the effective date (September 23, 2013) to become compliant with its changes to the Privacy, Security, and Breach Notification Rules.[3] The changes to the Enforcement Rule, however, are effective upon the effective date of the Final Rule.[4] Lastly, the Final Rule generally extends a significant grandfather period to business associate agreements ("BAA") that were in effect as of January 25, 2013, if: (1) such agreements are in compliance with the existing Privacy and Security Rules, and (2) are not renewed or modified from March 26, 2013, until September 23, 2013.[5] HHS has deemed such unmodified/non-renewed pre-Final Rule publication

---

[1] 75 Fed. Reg. 40868 (July 14, 2010).

[2] 78 Fed. Reg. 5566 (January 25, 2013).

[3] *Id.* at 5566.

[4] *Id.* at 5669.

[5] *Id.* at 5603 (to be codified at 45 C.F.R. § 164.532(e)(1)).

date BAAs to be compliant until the earlier of the date of renewal/modification or September 22, 2014 (i.e., one year subsequent to the general compliance date).

A. Enforcement Rule

The Final Rule adopts wholesale the modifications to the HIPAA Enforcement Rule set forth in HHS' Interim Final Rule of October 30, 2009 (the "IFR") and in the Proposed Rule. While what was set forth in the Proposed Rule did not change, public comments on the IFR and HHS' responses to those comments in the preamble to the Final Rule highlight enforcement issues that will likely pose significant challenges to covered entities and their business associates.

1. The HITECH Act

Section 13410 of the HITECH Act made important changes to HIPAA's enforcement and penalty scheme. Some of these changes took effect immediately upon enactment of the HITECH Act (February 18, 2009), while others were delayed until February 18, 2010 or later. Notably, Section 13410(d) applied to HIPAA violations occurring after the enactment date and established the following four categories of violations that reflect increasing culpability and civil monetary penalties (CMPs) associated with a violation:

- The first, and lowest, tier is for violations in which the person did not know, and, by exercising due diligence, would not have known that he or she violated a provision of the statute;
- The second tier is for violations due to reasonable cause and not willful neglect;
- The third tier is for violations that were due to willful neglect but were timely corrected; and
- The fourth tier is for violations that were due to willful neglect and were not timely corrected.

2. The IFR and the Proposed Rule

The IFR revised the Enforcement Rule to incorporate the provisions of Section 13410(d) outlined above and set the following penalty ranges for violations falling in the first three tiers, respectively: $100 to $50,000; $1,000 to $50,000; and $10,000 to $50,000. It also set a minimum penalty of $50,000 for each violation of the fourth tier, as well as a maximum aggregate penalty of $1.5 million annually for all violations of the same requirement or prohibition under any of the four categories. Finally, the IFR prohibited the imposition of penalties for any violation not involving willful neglect that is timely corrected.[6]

The Proposed Rule, in turn, proposed additional modifications to the Enforcement Rule to reflect other provisions of Section 13410 that took effect on or after February 18, 2010. These additional modifications included:

- Requiring that the Secretary formally investigate complaints indicating violations due to willful neglect and impose mandatory CMPs upon finding such violations;
- Amending the definition of "reasonable cause" as used in the second tier of violations to make clear that it encompasses instances in which a covered entity has knowledge of a violation, but lacks the conscious intent or reckless indifference associated with the third and fourth tiers of violations;

[6] 74 Fed. Reg. 56123, 56126–29 (October 30, 2009).

- Making business associates directly liable for CMPs for violations of certain HIPAA provisions;
- Requiring the Secretary to determine CMP amounts based upon the nature and extent of the harm resulting from a violation; and
- Barring the Secretary's authority to impose a CMP only to the extent a criminal penalty has actually been imposed with respect to an act under Section 1177 of the Social Security Act, rather than in cases in which the act constitutes an offense that is merely criminally punishable under that statutory section.

3. The Final Rule

The following issues elicited both public comment and more detailed responses from HHS in the preamble to the Final Rule.

a. Noncompliance Due to Willful Neglect

The Final Rule provides that the Secretary must now formally investigate a complaint or perform a compliance review if a preliminary investigation of the facts indicates a possible violation of the HIPAA rules due to willful neglect. In response to comments that such investigations and compliance reviews should be triggered only when the facts indicate a *probable* violation, HHS emphasizes that the HITECH Act envisioned mandatory inquiry in cases of possible willful neglect violations and that this approach strengthens enforcement with respect to such serious potential transgressions of the HIPAA rules.[7] Consistent with this position, HHS stresses that it is also adopting its earlier proposal to give itself discretion to move directly to imposing a CMP, without first exhausting informal resolution efforts, particularly in cases of more serious violations.[8]

Complaint Investigations and Compliance Reviews. In response to commenters' concerns about duplicative investigations and reviews conducted by the Secretary, HHS clarifies in the Final Rule that it generally conducts compliance reviews to investigate allegations of violations brought to HHS' attention through a mechanism other than a complaint (e.g., through a media report). *See* 78 Fed. Reg. at 5579.

b. Agency Relationships

Over the objections of various commenters, the Final Rule makes covered entities liable for the acts of their business associate "agents," and the latter liable for the acts of their subcontractor "agents," in accordance with the federal common law of agency and regardless of whether the covered entity has a compliant BAA in place. In the Final Rule, HHS does agree to provide additional guidance as to principal/agency liability in the context of covered entities, business associates, and subcontractors.[9] Importantly, not every business associate or subcontractor is an "agent" of the applicable covered entity or business associate, respectively. HHS' guidance stresses that determining whether a business associate is the agent of a covered entity is fact specific, and takes into account the terms of the BAA as well as the totality of the circumstances of the relationship between the two entities.[10] The same is true in assessing whether a subcontractor is the agent of a business associate.

---

[7] 78 Fed. Reg. at 5578–79 (to be codified at 45 C.F.R. §§ 160.306(c), 160.308)..

[8] *Id*. at 5579.

[9] *Id.* at 5580–81 (to be codified at 45 C.F.R. § 160.402(c)).

[10] *Id.* at 5581.

While various other factors are relevant, the key question is one of control.[11] If a covered entity can only control its business associate by amending the agreement between the two, or alleging a breach of that agreement, it's unlikely that an agency relationship exists. On the other hand, if the agreement between the parties gives the covered entity access to the protected health information ("PHI") being used by the business associate, as well as the right to give interim instruction and direction to the business associate during the course of their business dealings, these facts would likely indicate an agency relationship. HHS emphasizes that an agency relationship can exist even if the covered entity does not control every aspect of the business associate's activities for the covered entity, and even if the covered entity does not choose to exercise a right to control to which it is entitled pursuant to its contract with the business associate.[12] At a minimum, this analysis should be considered when determining the negotiated amount of time within which a business associate must notify a covered entity of a breach discovered by the business associate, as the Breach Notification Rule deems breaches discovered by covered entity's agent to have been discovered by the covered entity itself.

c. Determination of Penalty Amounts

In addition to retaining the penalty tiers and dollar ranges per violation set forth in the IFR and Proposed Rule (discussed above), HHS also clarifies how it will count the number of violations for purposes of calculating a CMP.[13] The agency provides three important guidelines:

- Where multiple individuals are affected by a use or disclosure, such as in the case of breach of unsecured PHI, the number of identical violations of the applicable Privacy Rule standard will be counted by the number of individuals affected;
- With respect to continuing violations, such as the lack of appropriate safeguards for a period of time, the number of identical violations will correspond to the number of days that the covered entity failed to have the safeguard in place; and
- With respect to applying the $1.5 million limit for identical violations in a calendar year to an enterprise with multiple business units, the limit applies to whatever legal entity constitutes a covered entity or business associate. That said, such a legal entity could theoretically be subject to multiple different violations, each allowing for the imposition of up to $1.5 million penalties, in the same calendar year.[14]

d. Penalty Factors

With regard to computing penalty amounts provided for by the HITECH Act, the Final Rule revises the factors that the Secretary is now *required* to consider. In particular, the Secretary will consider "reputational harm" in determining the nature and extent of the relevant harm resulting from a violation, as well as a covered entity's history of compliance.[15] As to reputational harm, HHS explains that this could arise not just from the unlawful disclosure of especially sensitive health information, such as records relating to sexually-transmitted diseases or mental health disorders, but also to information that in a specific case could adversely affect an individual's

---

[11] *Id.*

[12] *Id.* at 5582.

[13] *Id.* at 5583 (discussing 45 C.F.R. § 160.404(b)).

[14] *Id.* at 5584.

[15] *Id.* at 5585 (to be codified at 45 C.F.R. § 164.408).

employment, standing in his or her community, or personal relationships.[16] As to the covered entity's history of compliance, HHS clarifies that this includes more broadly "indications of noncompliance," and not simply "prior violations of HIPAA." Therefore, HHS' inquiry is not limited to findings of formal "violations," which HHS contends likely would not yield an accurate picture of a covered entity's or business associate's actual general compliance history.[17] This is the case because HHS uses various other tools besides formal violations findings to police covered entities, including informal resolutions of noncompliance through corrective action plans.

e. Cure Period for Violations

Under the HITECH Act and the IFR, a covered entity that corrects a violation due to willful neglect within 30 days of discovery could face a penalty of as little as $10,000, as opposed to the mandatory $50,000 penalty for a "fourth tier" violation if not timely corrected.[18] The 30-day cure period begins as of the day HHS *deems*, based on the evidence it gathers in its investigation, that the covered entity had "actual or constructive knowledge" of the violation.[19] In the Final Rule, HHS rejects commenters' suggestions that the cure period should begin after HHS notifies the covered entity of the violation. According to commenters, the existing standard leads to uncertainty as to when the period actually begins and that a business associate "agent's" knowledge could be imputed to the covered entity even before the business associate has informed the covered entity of the violation.[20]

In retaining the existing standard, HHS explains it is already compromising by not starting the 30-day cure period until the covered entity has "actual or constructive knowledge" of the violation, as opposed to starting it – as other laws often do – when the covered entity has knowledge of merely the facts underlying the violation.[21] The agency also stresses that its approach creates an appropriate incentive, which would be missing if the cure period were triggered solely based on an external notification, for the covered entity to establish a compliance program and self-correct. Finally, HHS explains that a business associate's knowledge of a violation would not likely be imputed to a covered entity if the business associate failed to notify the covered entity of the violation; a covered entity is only liable for the acts of its agent undertaken "within the scope of the agency," and a business associate that fails to provide such notice would likely be acting outside the scope of its agency.[22]

B. Impact on Business Associates

Arguably the most significant aspect of the Final Rule's change to the overall scope and application of HIPAA's implementing regulations, the Final Rule dramatically (though certainly expected in light of the Act's directives) extends to business associates the requirement to comply directly with the Security Rule and significant aspects of the Privacy Rule. Additionally, HHS made certain definitional changes and clarifications with regard to which individuals and entities qualify as a business associate.

---

[16] *Id.* at 5585.

[17] *Id.*

[18] *See* 45 C.F.R. § 164.410.

[19] 78 Fed. Reg. at 5587.

[20] *Id.*

[21] *Id.*

[22] *Id.*

1. Expanded Definition

The Final Rule significantly expands the definition of business associate to include health information organizations, e-prescribing gateways, and other entities that facilitate data transmission services to a covered entity and require access to PHI on a routine basis.[23] Significantly, the preamble to the Final Rule includes a potentially far-reaching discussion of the "conduit" exception (often referred to as the "common carrier" exception) and the government's view of when certain types of vendors qualify as a business associate. In declaring that the conduit exception should be narrowly construed, HHS clarifies (both in the preamble and definition of business associate itself) that "an entity that maintains protected health information on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the protected health information."[24] Additionally, the Final Rule includes in the expanded definition of business associate entities that offer a personal health record on behalf of a covered entity.

2. Subcontractors

The Final Rule's expansion of the definition of business associate is most dramatically reflected in its inclusion of business associate subcontractors as actual business associates. As a result of this change, a business associate's subcontractors (and subcontractors of a subcontractor, all the way down the chain) will be regulated in the same manner as any other business associate under the Final Rule, provided that the subcontractor has been delegated a function, activity, or service that involves the creation, receipt, maintenance, or transmission of PHI.[25]

3. Direct Liability

Under the HITECH Act and the Final Rule, business associates and subcontractors are directly liable for CMPs under the HIPAA Privacy Rule for "impermissible uses and disclosures of PHI," which include violations of the minimum necessary rule, as well as the following HITECH requirements:

- For a failure to provide breach notification to the covered entity;
- For 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 BAA);
- For a failure to disclose PHI where required by the Secretary to investigate or determine the business associate's compliance with the HIPAA Rules;
- For a failure to provide an accounting of disclosures; and
- For a failure to comply with the requirements of the Security Rule.[26]

While "impermissible uses and disclosures of PHI" include any use or disclosure that would violate the Privacy Rule if done by a covered entity, it is the Business Associate Agreement and Business Associate Subcontractor

---

[23] *Id.* at 5571.

[24] *Id.* at 5572; *see* 45 C.F.R. § 160.103 (defining "Business Associate").

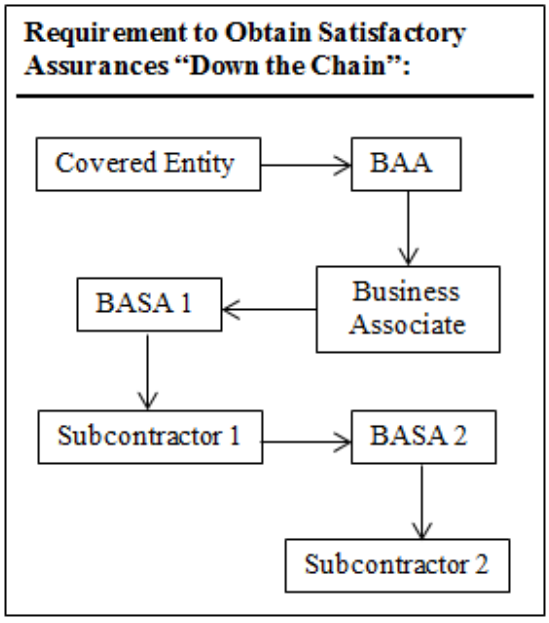
[25] 78 Fed. Reg. at 5572.

[26] 78 Fed. Reg. at 5598–99, 5601.

Agreement that "clarify and limit, as appropriate, the permissible uses and disclosures" of PHI by business associates and subcontractors. Therefore, the HITECH Act and the Final Rule tie much of "business associate [direct] liability to making uses and disclosures in accordance with the uses and disclosures laid out in such agreements, rather than liability for compliance with the Privacy Rule generally."[27]

a. The Privacy Rule and Direct Liability under Business Associate Agreements and Business Associate Subcontractor Agreements (BASAs)

Under Section 13404(a) of the HITECH Act and the Final Rule, business associates become directly liable for uses and disclosures of PHI that do not comply with the business associate's or subcontractor's BAA or BASA, respectively. Stated differently, effective September 23, 2013, a business associate that breaches its BAA is contractually liable to the applicable covered entity and may be directly liable to HHS. Interestingly, however, direct liability to HHS is not dependent upon the actual existence of a BAA or BASA—"liability for impermissible uses and disclosures attaches immediately when a person creates, receives, maintains, or transmits protected health information on behalf of a covered entity or business associate and otherwise meets the definition of a business associate."[28] Therefore, while the BAA may clarify and limit permissible uses and disclosures of PHI, business associates are still prohibited from using and disclosing PHI in a manner that would violate the Privacy Rule if done by a covered entity regardless of the existence of a BAA.



HHS received many comments questioning whether covered entities are required to obtain satisfactory assurances in the form of a BASA from a business associate's subcontractor. The Final Rule makes clear that a covered entity is not required to enter into a contract or other arrangement with a business associate that is a subcontractor. Rather, as illustrated by the diagram to the right, it is the obligation of the business associate that has engaged the subcontractor to enter into a BASA.[29]

Interestingly, as stated above, whether a person is a business associate depends upon whether that person creates, receives, maintains or transmits PHI on behalf of a covered entity and not on whether the person has entered into a BAA with the covered entity. Therefore, a business associate's obligation to enter into a BASA is triggered when the business associate engages a subcontractor to create, receive, maintain, or transmit PHI on behalf of the business associate. That obligation exists regardless of whether the covered entity has met its obligation of requiring the business associate to enter into a BAA.[30]

---

[27] *Id.* at 5601.

[28] *Id*. at 5598.

[29] *Id.* at 5573, 5590, 5601.

[30] *See id.* at 5697 (outlining the new requirements at 45 C.F.R. §§ 164.502(e)(1) and (2)).

b. The Security Rule and Direct Liability

The Final Rule adopts the HITECH Act's provisions extending direct liability for compliance with the Security Rule to business associates. While BAAs executed prior to January 25, 2013, do not need to become HITECH-compliant until the earlier of September 23, 2014 or when the BAA is renewed or modified,[31] beginning September 23, 2013, business associates (which includes subcontractors) must comply with, and are directly liable for violations of, the Security Rule's administrative, physical, and technical safeguards requirements in Sections 164.308, 164.310, and 164.312, as well as the Rule's policies and procedures and documentation requirements in Section 164.316. Such requirements include performing a Security Rule risk assessment (which has been the trigger for multiple recent HHS enforcement actions), establishing a risk management program, and designating a security official.[32]

In response to comments regarding the cost of compliance for both traditional/prime business associates and subcontractors, HHS reminds business associates of their current obligations under BAAs that comply with the existing Privacy and Security Rules: business associates must (1) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the business associate creates, maintains, or receives, and (2) require their agents (and subcontractors) to implement reasonable and appropriate safeguards as well. Therefore, HHS expects only "modest improvements" are likely necessary for business associates and subcontractors to come into compliance. The requirements of the Security Rule also remain flexible and scalable, and business associates may choose security measures that are appropriate for their size, resources, and the nature of the security risks they face.[33]

C. Breach Notification Rule

With regard to the existing regulatory exceptions to what constitutes a breach, as well as the mechanics of notifications and associated obligations under the 2009 interim final Breach Notification Rule, the Final Rule serves merely as a clarifying document. The Final Rule does, however, make one far reaching and extremely significant change to the interim final rule – the removal of the risk of harm assessment.[34]

1. Presumption of Breach/Risk of Harm Assessment Replaced

The Final Rule explicitly provides that impermissible uses or disclosures of PHI will be presumed to be a breach unless the associated covered entity or business associate demonstrates that there is a "low probability that the protected health information has been compromised."[35] Because the determination of risk of harm to an individual under the interim final rule's standard often proved challenging – particularly with regard to determination of reputational harm – HHS replaced the risk of harm assessment with a four-pronged, "more objective" test. Though refusing to implement a bright line standard as to what qualifies as a breach, the Final Rule requires covered entities and business associates to consider the following factors (along with any other relevant considerations) designed to "focus more objectively on the risk that the protected health information has

---

[31] *Id.* at 5603.

[32] *Id.* at 5569, 5589.

[33] *Id.* at 5589.

[34] *Id.* at 5641.

[35] *Id.*

been compromised" as compared to the significant risk to an individual caused by the impermissible use or disclosure:

- The nature and extent of the PHI involved, including types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the PHI or to whom it was disclosed (if the person to whom the PHI was improperly disclosed is another covered entity or someone obligated to protect PHI, this would favor a determination that there is a low probability that the PHI was compromised).
- Whether the PHI was actually acquired or viewed (if, for example, a laptop containing unencrypted PHI is lost, but later found and forensic analysis reveals that the PHI was never accessed, this would favor a determination that no notification is required).
- The extent to which the risk to the PHI has been mitigated (if PHI is improperly used or disclosed, the covered entity or business associate should immediately take steps to mitigate any potential risk to the PHI, which would favor a determination that there is a low probability that the PHI was compromised).[36]

Although the Final Rule's preamble discussion highlights the above factors' replacement of the risk of harm assessment as an attempt to ensure a more objective and uniform application of the rule, discussion associated with the first of the four new factors does specifically address the need for covered entities and business associates to consider "whether the [impermissible] disclosure involved information . . . is of a more sensitive nature."[37] Furthermore, HHS clarifies that such sensitive information includes more than PHI addressing sexually transmitted diseases, mental health conditions, or substance abuse treatment. This appears to suggest that whether PHI has been "compromised" will still require some consideration of the risk of harm to the individual albeit within the confines of the Final Rule's new overall approach to analyzing a breach of unsecured PHI.

An Individual's Right to Request Access to Electronic PHI via an Unencrypted Email. In order to comply with an individual's right to request an electronic copy of PHI (see Section J.2 below), covered entities are permitted to send individuals unencrypted emails *if* they have advised the individual of the risk, and the individual still prefers the unencrypted email. In such circumstances, covered entities are not responsible for unauthorized access of PHI while in transmission to the individual based on the individual's request and are not responsible for safeguarding information once delivered to the individual. *See* 78 Fed. Reg. at 5634.

2. Significant Clarifications

The Final Rule removes the interim final Breach Notification Rule's exception relating to an impermissible disclosure of PHI involving only a limited data set that also excludes dates of birth and zip codes.[38] Instead, such potential breaches should be analyzed under the Final Rule's new standard.

In terms of the annual notifications that covered entities must make to HHS regarding each calendar year's breaches involving fewer than 500 individuals (which may be made within 60 days after the end of applicable calendar

[36] *Id.* at 5642.

[37] *Id.*

[38] *Id.* at 5644.

year), HHS clarifies that the trigger for such notification is the date of a breach's discovery as opposed to the date on which the incident occurred.[39]

Clarifying an ambiguous aspect of the interim final rule's media notice requirement, HHS makes it clear that a covered entity is not required to incur any cost to print or run the media notice. Instead, it is permissible to fulfill this obligation through the issuance of a press release.[40]

Lastly, emphasizing that the timing requirement for notification is truly "without unreasonable delay," HHS warns that, depending on the facts and circumstances associated with a particular breach, notification may be viewed as late even if it comes within 60 calendar days of the discovery of the breach.[41]

D. Notice of Privacy Practices

The Final Rule mandates the inclusion of several additional statements in a covered entity's Notice of Privacy Practices ("NPP"), which triggers a covered entity's obligation under the existing Privacy Rule to redistribute its revised NPP.

1. New Required Statements Regarding Authorizations

The Final Rule requires that a covered entity's NPP include a statement indicating that the following uses and disclosures require authorization from the individual:

- Most uses and disclosures of psychotherapy notes (where appropriate);
- Uses and disclosures of PHI for marketing purposes; and
- Uses and disclosures that constitute a sale of PHI.[42]

The Final Rule clarifies that with respect to psychotherapy notes, an NPP need not include a description of the covered entity's recordkeeping practices (although covered entities are free to do so). In addition, covered entities that do not maintain psychotherapy notes are not required to include a statement regarding authorizations for psychotherapy notes in their NPPs.[43]

Perhaps more importantly, in addition to the uses and disclosures described above, an NPP must now contain a statement that other uses and disclosures *not described in the NPP* will be made only with an authorization from the individual.[44]

---

[39] *Id.* at 5654.

[40] *Id.* at 5653.

[41] *Id.* at 5648.

[42] *Id.* at 5624 (to be codified at 45 C.F.R. § 164.520(b)(1)(ii)(E)).

[43] *Id.* at 5624.

[44] *Id.* at 5624 (to be codified at 45 C.F.R. § 164.520(b)(1)(ii)(E)).

2. Additional Required Statements

a. Fundraising Communications

If a covered entity intends to contact an individual in support of its fundraising activities, the covered entity must include in the NPP a statement informing the individual of this intention and that the individual has the right to opt out of receiving such communications.[45] The Final Rule clarifies that this statement need not include the mechanism for individuals to opt out of receiving fundraising communications, but that covered entities are free to include such information in their NPPs.[46] Individuals must continue to receive an opportunity to opt out with each solicitation. For a more detailed discussion of how fundraising communications are treated under the Final Rule, see Section I below.

b. Genetic information

If a covered entity is a health plan that underwrites (except certain long-term care plans) and intends to use or disclose PHI for underwriting purposes, the covered entity must include a statement in its NPP informing the individual that the plan cannot use genetic information for such purposes.[47]

In addition to changes to NPPs mandated by GINA, HHS amends the Privacy Rule to:

- Explicitly provide that genetic information is health information for purposes of the Privacy Rule.
- Prohibit all covered health plans, except issuers of long-term care policies, from using or disclosing protected health information that is genetic information for underwriting purposes.

In order to clarify and properly implement the new GINA provisions, the Final Rule also adopts or modifies the following definitions: (i) Health Information; (ii) Genetic Information; (iii) Genetic Test; (iv) Genetic Services; (v) Family Member; (vi) Manifestation (or Manifested); (vii) Health Plan; (viii) Underwriting Purposes; (ix) Health Care Operations; and (x) Payment.

c. Individual's Right to Request a Required Restriction

Consistent with the Act and Proposed Rule, and as outlined in more detail below in Section J.1, the Final Rule requires that covered entities comply with an individual's request to restrict disclosure of the individual's PHI to a health plan where the disclosure (a) is for payment or health care operations purposes, and (b) pertains to a health care item or service for which the individual has paid the covered entity in full. The Final Rule also requires that covered entities include a statement in their NPP regarding this limited right to request required restrictions. [48]

d. Breach Notification Obligations

Covered entities must include in their NPP a statement that covered entities are required to notify affected individuals following a breach of unsecured PHI.[49] The Final Rule clarifies that a simple statement in the NPP that an individual has a right to receive notifications of breaches of unsecured PHI will suffice. Such a statement need not describe how the covered entity will determine whether a breach has occurred, or include the regulatory descriptions of "breach" or "unsecured PHI," or even describe the types of information to be provided in the actual breach notification to the

---

[45] *Id.* at 5624 (to be codified at 45 C.F.R. § 164.520(b)(1)(iii)(A)).

[46] *Id.* at 5624.

[47] *Id.* at 5625 (to be codified at 45 C.F.R. § 164.520(b)(1)(iii)(C)).

[48] *Id*. at 5624 (to be codified at 45 C.F.R. § 164.520(b)(1)(iv)(A)).

[49] *Id*. at 5624 (to be codified at 45 C.F.R. § 164.520(b)(1)(v)(A)).

individual.[50] See Section C, above, for a more detailed discussion of the Final Rule's changes to the Breach Notification Rule.

3. Required Changes to NPP Trigger Redistribution Obligations

The Final Rule states that the required revisions to NPPs represent "material changes" so as to trigger covered entities' distribution obligations, which vary for covered entity plans and providers.[51]

a. Health Care Providers

For covered entity providers, the Final Rule does not modify the current requirements to distribute revisions to the NPP. As such, providers must make the revised NPP available upon request on or after the effective date of a revision (e.g., subsequent to September 23, 2013).[52] The Final Rule does, however, provide important clarifications to the distribution requirements under the existing Privacy Rule.

The Final Rule clarifies that providers are not required to print and hand out a revised NPP to all individuals seeking treatment. Rather, providers must post the revised NPP in a clear and prominent location and have copies of the NPP at the delivery site for individuals to request to take with them. With respect to new patients, NPP distribution obligations have not changed.[53]

The Final Rule also clarifies that while health care providers are required to post the NPP in a clear and prominent location at the delivery site, providers may post a summary of the NPP in such a location as long as the full NPP is immediately available for individuals to pick up without any additional burden on their part (e.g., placing the full NPP on a table directly under the posted summary). HHS explicitly warns that requiring an individual to request a copy of the full NPP from a receptionist "would not be appropriate."[54]

b. Health Care Plans

A health care plan that currently posts its NPP on its website must: (1) prominently post the material change or its revised notice on its website by the effective date of the material change to the notice; and (2) provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan.[55]

A health care plan that does not have a customer service website must provide the revised NPP, or information about the material change and how to obtain the revised notice, to individuals covered by the plan within 60 days of the material revision to the notice.[56]

---

[50] *Id.* at 5624.

[51] *Id.*

[52] 45 C.F.R. § 164.520(c)(2)(iv).

[53] 78 Fed. Reg. at 5624.

[54] *Id.*

[55] 45 C.F.R. § 164.520(e)(2)(v)(A).

[56] *Id.*

E. Authorizations

The Final Rule significantly alters the regulations that govern the use or disclosure of PHI for which a covered entity must obtain an authorization, and imposes additional burdens on covered entities and business associates that market or sell PHI. At the same time, certain requirements governing authorizations for the use or disclosure of PHI for research purposes have been relaxed. New (and revised) rules governing the uses and disclosures of PHI for marketing purposes, the sale of PHI, and the use of PHI for research purposes (and corresponding requirements for authorizations permitting such uses and disclosures) are outlined below in Sections F, G, and H.

Required Authorizations. Pursuant to the Final Rule, there are three circumstances in which an authorization from an individual must be obtained:

- The sale of PHI;
- Uses and disclosures of PHI for marketing purposes; and
- Most uses and disclosures of psychotherapy notes.

See 78 Fed. Reg. at 5699.

Nevertheless, the Final Rule does not alter the content of the Privacy Rule's core elements and required statements that are outlined in 45 C.F.R. § 164.508(c). Thus, the substance of a HIPAA-compliant authorization for the use or disclosure of PHI largely remains intact.

F. Marketing

1. Financial Remuneration and Treatment and Health Care Operations Communications

In a marked departure from the Proposed Rule's approach to marketing, the Final Rule requires authorizations for all health care operations *and treatment* communications where the covered entity receives financial remuneration for making the communication from a third party whose products or services are being described.[57] Under the existing Privacy Rule, treatment and certain health care operations communications were specifically excluded from the definition of "marketing."[58] Those same exceptions are no longer applicable if in exchange for making the communication, the covered entity receives financial remuneration from a third party.

Marketing and Business Associates. Because the Privacy Rule provides that a business associate agreement may not authorize the business associate to further use or disclose PHI in a manner that would violate the Privacy Rule if done by the covered entity, an authorization is also required where a business associate (including a subcontractor) receives financial remuneration from a third party in exchange for making a communication about a product or service. *See* 45 C.F.R. § 164.504(e)(2)(i).

"Financial remuneration" is defined as "direct or indirect payment from or on behalf of a third party whose product or service is being described," but does not include payments for the actual treatment of the individual. Indirect payments refer to payments that flow from an entity on behalf of the third party whose product or service is being described to the covered entity. Notably, financial remuneration does not include non-financial, *in-kind* benefits; instead, it is limited to actual *monetary* payments.[59] For example, a third party may provide a covered entity with *in-kind* goods, such as written materials, that describe the third party's products or services. The covered entity may then distribute those materials to its patients for the purpose of recommending the third party's product or service as an alternative treatment without obtaining an authorization. By contrast, if the covered entity also receives a

[57] 78 Fed. Reg. at 5595.

[58] 45 C.F.R. § 164.501 (defining "marketing").

[59] 78 Fed. Reg. at 5595–96 (to be codified at 45 C.F.R. § 164.501(defining "marketing")).

monetary payment from the third party for the purpose of making the communication, then an authorization is required.

Importantly, for financially remunerated treatment and health care operations communications that will require an authorization under the Final Rule, the scope of the authorization need not be limited to communications describing a single product or service or the products or services of a single third party. Instead, authorizations may apply to subsidized communications generally, provided that the authorization adequately describes the intended purposes of the requested uses and disclosures. Such authorizations must also disclose the fact that the covered entity is receiving financial remuneration from a third party.[60]

Going forward, covered entities will need to answer two important questions prior to using or disclosing PHI for treatment or health care operations communications that involve the receipt of financial remuneration from a third party: (1) whether the covered entity is receiving "financial remuneration" as defined by the Privacy Rule, and (2) whether the covered entity is receiving the financial remuneration for the purpose of making the communication.

Exceptions to the Authorization Requirement for Marketing Communications under the Existing Privacy Rule Remain. Regardless of whether a covered entity receives financial remuneration from a third party to make a treatment or health care operations communication (or other marketing communication), if the communication is made face-to-face or consists of a promotional gift of nominal value, then no authorization is required. *See* 45 C.F.R. § 164.508(a)(3)(i).

2. Prescription Refill Reminders

As expected, HHS includes the statutory exception to the definition of "marketing" for communications about a "drug or biologic that is currently being prescribed" to the individual in the Final Rule, as well as regulatory text that expressly includes prescription refill reminders within that exception.[61] While HHS intends to provide further guidance on the scope of the exception, it clarifies in the Final Rule that the following communications are included within the exception:

- Communications regarding generic equivalents of a currently prescribed drug;
- Communications that encourage individuals to take their prescribed medication as directed; and
- For individuals who are prescribed a self-administered drug or biologic, communications regarding all aspects of a drug delivery system.[62]

While a covered entity may receive financial remuneration in exchange for making these communications and still remain within the marketing exception, such remuneration must be limited to the covered entity's costs for making the communication. Permissible costs include only the costs of labor, supplies, and postage. Where a covered entity generates a profit or receives payment for other costs in exchange for making a prescription refill reminder, the exception would not apply and the covered entity must obtain individual authorization prior to using or disclosing PHI in furtherance of the communication.[63]

---

[60] *Id.* at 5596.

[61] *Id.* at 5596–97 (to be codified at 45 C.F.R. § 164.501(defining "marketing")).

[62] *Id.* at 5596.

[63] *Id.* at 5596–97.

G. Sale of Protected Health Information

The HITECH Act and Final Rule generally prohibit the sale of PHI by a covered entity or business associate unless the covered entity or business associate obtains an authorization from the individual in compliance with the new Section 164.508(a)(4).[64] There are important exceptions to this prohibition and, therefore, the authorization requirement. However, some of these exceptions are limited to those disclosures where the remuneration received by the covered entity or business associate includes *only* a reasonable cost-based fee to cover the costs to prepare and transmit the PHI.

1. Sale of PHI Defined

HHS defines the "sale of PHI" to a mean a disclosure of PHI by a covered entity (or business associate, if applicable) where the covered entity directly or indirectly receives "remuneration" from or on behalf of the recipient of the PHI in exchange for the PHI.[65] In addition to financial payments, the term "remuneration" includes nonfinancial benefits, such as in-kind benefits. Importantly, HHS does not limit a "sale" to those transactions where there is a transfer of ownership of PHI; the sale of PHI provisions apply equally to disclosures in exchange for remuneration including those that are the result of access, license, or lease agreements.[66]

Notably, HHS does not consider the sale of PHI to encompass payments a covered entity may receive in the form of grants or contracts to perform programs or activities, including research activities, even if the covered entity is required to report PHI-containing results as a condition of receiving the funding. In such circumstances, the covered entity is not receiving remuneration in exchange for disclosing PHI, but is instead receiving remuneration to perform the program or research activity. By contrast, a sale of PHI occurs when the covered entity primarily is being compensated to supply PHI it maintains in its role as a covered entity (or a business associate).[67]

The Role of (Financial) Remuneration under Marketing versus Sale of PHI Provisions. Unlike the marketing provisions discussed above, which are limited to the receipt of *financial payments*, "remuneration" as applied in the sale of PHI provisions *is not limited to financial payments* and therefore is applicable to the receipt of nonfinancial as well as financial benefits. *See* 78 Fed. Reg. at 5607.

2. Exceptions

The sale of PHI prohibition and authorization requirement is not applicable to the following situations where the covered entity or business associate receives remuneration in exchange for disclosing PHI:

- For public health purposes;
- For treatment and payment purposes;

---

[64] *See* Section 13405(d) of the HITECH Act; 78 Fed. Reg. at 5606 (to be codified at 45 C.F.R. § 164.502(a)(5)(ii)(A)).

[65] 78 Fed. Reg. at 5606 (to be codified at 45 C.F.R. § 164.502(a)(5)(ii)(B)).

[66] *Id.* at 5606.

[67] *Id.*

- For the sale, transfer, merger or consolidation of all or part of the covered entity and for related due diligence; and

- As required by law.

The remuneration received for the above exceptions *is not limited* to a covered entity's or business associate's reasonable costs to prepare and transmit the PHI. By contrast, the exceptions outlined below do include various limitations on the type of remuneration a covered entity or business associate may receive:

- For research purposes.

To be within the exception, a covered entity or business associate may only receive a reasonable cost-based fee to cover the cost to prepare and transmit the PHI. HHS also clarifies that a reasonable cost-based fee may include both direct and indirect costs, including labor, materials, and supplies for generating, storing, retrieving, and transmitting the PHI; labor and supplies to ensure the PHI is disclosed in a permissible manner; as well as related capital and overhead costs. However, if a covered entity or business associate incurs a profit from the PHI disclosure for research purposes, then the exception is not applicable and an authorization is required.

Importantly, and as discussed further below, if a covered entity or business associate incurs a profit for disclosing PHI for research purposes, an Institutional Review Board ("IRB") or Privacy Board waiver to the authorization requirement in compliance with Section 164.512(i) is no longer sufficient.

- To the individual to provide the individual with access to PHI or an accounting of disclosures.

Limitations on the fees a covered entity or business associate may charge as set out in Sections 164.524 and 164.528 still apply for a disclosure of PHI to qualify for the exception.

- To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor.

Such remuneration provided by a covered entity to a business associate (or by a business associate to a subcontractor) must be for the actual performance of the activities that the business associate (or subcontractor) undertakes on behalf of a covered entity (or business associate).

- For any other purpose permitted by or in accordance with the Privacy Rule.

Similar to the research exception discussed above, to be within this exception, a covered entity or business associate may only receive a reasonable cost-based fee to cover the cost to prepare and transmit the PHI.[68]

[68] *Id.* at 5607–09 (to be codified at 45 C.F.R. § 164.502(a)(5)(ii)(B)(2)).

H. Research

1. Compound Authorizations

As an exception to the Privacy Rule's general prohibition on conditioning treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of an authorization, covered entities may condition the provision of research-related treatment (e.g., a clinical trial) on obtaining the individual's authorization for the use or disclosure of PHI for such research.[69]

Revocation of Compound Authorizations. Where it is clear that an individual is revoking only part of a compound research authorization, such revocation does not equate to a revocation of the entire authorization. However, where it is not clear to which research activities the revocation applies, written clarification must be obtained from the individual or the entire authorization must be treated as revoked. *See* 78 Fed. Reg. at 5611.

The Privacy Rule also generally prohibits "compound authorizations," which occur when an authorization for the use and disclosure of PHI is combined with any other legal permission. However, as an exception to this general prohibition, the Privacy Rule permits "compound authorizations" for research purposes, such that an authorization for a research study may be combined with any other written permission for the same study, including another authorization or informed consent to participate in the research.[70] Despite this exception, prior to the Final Rule, the Privacy Rule prohibited combining an authorization that conditions treatment, payment, enrollment in a health plan, or eligibility for benefits ("conditioned authorization") with an authorization for another purpose for which treatment, payment, enrollment, or eligibility may not be conditioned ("unconditioned authorization").[71] In the research environment, this limitation on compound authorization has resulted in inconsistency with the Common Rule (45 C.F.R. Part 46). For example, covered entities were required to obtain separate authorization from research participants for a clinical trial that also collected specimens with associated PHI for a central tissue repository.

The Final Rule amends the limitation on compound authorizations to allow a covered entity to combine conditioned and unconditioned authorizations for research, so long as the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities.[72] Compound authorizations that only allow the individual to opt out of the unconditioned authorization are not permitted.[73] Covered entities have the flexibility to determine how they will meet the authorization requirements, but must include the core elements and statements required for a valid authorization, which as stated above, have not substantively changed pursuant to the Final Rule.

---

[69] 45 C.F.R. § 164.508(b)(4)(i).

[70] *Id.* at § 164.508(b)(3)(i).

[71] *Id.* at § 164.058(b)(3)(iii).

[72] 78 Fed. Reg. at 5610.

[73] *Id.*

Grandfathering of Existing Consents, Authorizations and IRB Waivers.

- Covered entities and researchers involved in existing, ongoing studies that involve the possibility of future research may rely on IRB-approved consent obtained prior to March 26, 2013 that reasonably informed individuals of the future research, provided that the informed consent was combined with a HIPAA-compliant authorization for the original study. *See* 78 Fed. Reg. at 5613.

- Covered entities may also rely on prior permissions (HIPAA-compliant authorizations or IRB waivers) obtained before September 23, 2013 to disclose PHI for research purposes even if remuneration in excess of the covered entity's reasonably cost is involved. *See* 78 Fed. Reg. at 5608.

2. Future Research

Research often involves obtaining a participant's health information or biological specimens for use in future research. The Common Rule permits researchers to use an informed consent form that seeks a participant's consent for the clinical trial as well as for future research that uses the participant's identifiable information or specimens.[74] HHS previously interpreted the Privacy Rule to require authorizations for research to be study specific, which was inconsistent with the Common Rule. While the Final Rule does not make any textual changes to the Privacy Rule in this regard, HHS does modify its interpretation of the Privacy Rule. Now, authorizations need not be study specific, provided that future uses or disclosures are sufficiently described to enable individuals to reasonably expect that their PHI could be used or disclosed for future research. [75] Additionally, the authorization must still contain the elements of a valid authorization, even if they are described in a more general manner than is done for specific studies.[76]

The changes to compound authorizations and future research streamline the research authorization process, which increases flexibility for, and decreases the burden on, covered entities. The changes also harmonize the Privacy Rule with the Common Rule.

3. Sale of PHI and Disclosures for Research Purposes

As described in detail above, under the Final Rule, authorization for the use or disclosure of an individual's PHI must be obtained for the sale of PHI. The Final Rule contains several exceptions to this authorization requirement, including where the purpose of the disclosure in exchange for remuneration is for research purposes.[77] However, the exception applies only when the covered entity receives a reasonable, cost based fee to prepare and transmit the information.[78]

Notably, the sale of PHI does not include payments a covered entity may receive in the form of grants, or contracts or other arrangements, to perform programs or activities, such as a

Authorization Waivers and Sale of PHI. The Privacy Rule permits covered entities to use and disclose PHI for research purposes without an authorization provided that a waiver is approved by an IRB or Privacy Board. However, even if a waiver is approved, an authorization for the sale of PHI is required if the covered entity gains a profit from the disclosure of PHI for research purposes. *See* 78 Fed. Reg. at 5608.

---

[74] 45 C.F.R. Part 46.

[75] 78 Fed. Reg. at 5612.

[76] *Id.* at 5613.

[77] *Id.* at 5606–07.

[78] *Id.*

research study, where any provision of PHI to the payer is a byproduct of the service being performed.[79] Therefore, the payment by a research sponsor to a covered entity to conduct a research study is not considered sale of PHI even if the study involves disclosing research results that include PHI to the sponsor. Conversely, a sale of PHI does exist where a covered entity is receiving remuneration from the recipient of the PHI for the information itself.

Because the research exception is a conditional exception, it may impose additional burdens on covered entities and/or researchers. To the extent covered entities agree to receive payment only for the costs to prepare and transmit the PHI, those entities would experience a loss of revenue.[80] Conversely, to the extent covered entities are not willing to accept payment only for the costs to prepare and transmit the data, researchers may incur additional costs in order to obtain the newly-required authorizations.[81]

I. Fundraising

Section 164.514(f) of the Privacy Rule permits a covered entity to use or disclose certain elements of an individual's PHI to make fundraising communications without obtaining the individual's authorization provided that certain requirements are met. Fundraising communications include communications made by the covered entity, an institutionally-related foundation, or a business associate on behalf of the covered entity for the purpose of raising funds for the covered entity.[82] Under Section 13406(b) of the HITECH Act, HHS must issue rules requiring that covered entities provide clear and conspicuous opportunities to recipients of fundraising communications to opt out of receiving future fundraising communications. Importantly, the revised rules do not require covered entities to send pre-solicitation opt out opportunities prior to the first fundraising communication.[83]

1. Additional Elements of PHI May Be Used or Disclosed for Fundraising Purposes

Under the existing Privacy Rule, covered entities may use or disclose only demographic information relating to the individual and dates of health care services provided to the individual for fundraising communications.[84] The Final Rule clarifies the scope of such demographic information to include name, address, other contact information, age, gender, and date of birth.[85] Additionally, the Final Rule expands the scope of the PHI that a covered entity may use or disclose to a business associate or institutionally-related foundation to include department of service, treating physician, and outcome information.[86]

2. New Requirements Governing Fundraising Communications

Under the existing Privacy Rule, a covered entity may not use or disclose PHI for fundraising purposes unless a statement is included in the covered entity's notice of privacy practice notifying the individual of the potential for

---

[79] *Id.* at 5606.

[80] *Id.* at 5679.

[81] *Id.*

[82] *Id.* at 5620–21.

[83] *Id.* at 5622.

[84] 45 C.F.R. § 164.514(f)(1).

[85] 78 Fed. Reg. at 5621.

[86] *Id.* at 5622 (to be codified at 45 C.F.R. § 164.514(f)(1)).

such communications. Now, as discussed above, that statement must also inform individuals of their right to opt-out of fundraising communications.[87] Additionally, the Final Rule enhances the requirements governing fundraising communications in four key aspects. More specifically, HHS replaces the standard that covered entities must make "reasonable efforts" not to send fundraising communications to individuals who opt out of such communications with the following new specifications:

- First, with each fundraising communication "made"—not just "sent"—to an individual, a covered entity must provide the individual with a "clear and conspicuous opportunity to elect not to receive any further fundraising communications." The revised standard is meant to apply to both written and oral communications. Importantly, although HHS gives a covered entity wide latitude to determine the method by which an individual may opt out of such communications, the method "may not cause the individual to incur any undue burden or more than a nominal cost."[88]

- Second, the regulation makes clear that a covered entity "may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications."[89]

- Third, a covered entity is prohibited from making fundraising communications to an individual where the individual has elected not to receive these communications "under paragraph (f)(1)(ii)(B) of this section."[90] Curiously, Section 164.514(f) does not contain a section (f)(1)(ii)(B), so we assume that HHS is referring to the opt out provision in Section 164.514(f)(2)(ii).

- Fourth, a covered entity is permitted—but not required—to provide a method for an individual who has previously opted out of receiving fundraising communications to opt back in.[91]

Importantly, the Final Rule balances HHS' attempts to provide strong protections for individuals who opt out of receiving fundraising communications with granting flexibility to covered entities to determine the scope of the opt out. Stated differently, a covered entity may limit an individual's opt-out to a specific fundraising campaign or apply the opt-out to all fundraising communications made by the covered entity.[92]

J. Individual Rights

Unfortunately (although not unexpected), the Final Rule does not address the new statutory requirements for accounting of disclosures of PHI for treatment, payment, and health care operations purposes, which were the subject of a May 2011 proposed rule and will be subject to future rulemaking.[93] The Final Rule does, however, revise an individual's right to restrict certain uses and disclosures of PHI, as well as to access their PHI to the extent such information is maintained in a designated record set.

---

[87] *Id.* at 5622 (to be codified at 45 C.F.R. §§ 164.514(f)(2)(i), 164.520(b)(1)(iii)(A)).

[88] *Id.*at 5622 (to be codified at 45 C.F.R. § 164.514(f)(2)(ii)).

[89] *Id.* at 5622 (to be codified at 45 C.F.R. § 164.514(f)(2)(iii)).

[90] *Id.*at 5621 (to be codified at 45 C.F.R. § 164.514(f)(2)(iii)).

[91] *Id.*at 5621 (to be codified at 45 C.F.R. § 164.514(f)(2)(v)).

[92] *Id.*at 5621.

[93] *Id.* at 5568.

1. Right to Request a Required Restriction

The Final Rule revises an individual's right to request certain restrictions on the uses and disclosures of the individual's PHI in light of new statutory requirements under HITECH.[94] Now, covered entities are *required to comply* with an individual's request to restrict disclosure of the individual's PHI to a health plan where (1) the disclosure is for payment or health care operations purposes and is not otherwise required by law, and (2) the PHI pertains solely to health care services or items for which the individual, or another person on the individual's behalf (other than a health plan), has paid the covered entity in full.[95]

Under the Existing Privacy Rule, while covered entities are not required to agree, an individual has the right to request a restriction on uses and disclosures of PHI: (1) to carry out treatment, payment, or health care operations, or (2) to family members and others involved in the individual's care. *See* 45 C.F.R. § 164.524.

a. "Required by Law" Exception

The "required by law" exception allows covered entities to disclose PHI to health plans for payment and health care operations purposes despite a requested restriction where another law compels the covered entity to make the disclosure and that obligation is enforceable in a court of law. This includes, for example, Medicare conditions of participation with respect to health care providers participating in the program, as well as state and other laws that require providers to submit a claim to a health plan for a covered service and provide no exception for individuals wishing to pay out-of-pocket for the service.[96]

Notably, a contractual requirement to submit a claim or otherwise disclose PHI to an HMO, as opposed to a requirement under state or other law, does not meet the "required by law" exception. Such provider contracts with HMOs must be renegotiated and updated prior to September 23, 2013 to be consistent with these new requirements under the Privacy Rule.[97]

b. Operational Concerns

To address many concerns regarding how to practically operationalize a restriction, HHS is relying on covered entities complying with existing minimum necessary policies and procedures, as well as on covered health care providers counseling their patients on the patient's obligations to ensure enjoyment of the right. Importantly, covered entities are not required to create separate medical records or otherwise segregate PHI subject to a restriction. Instead, HHS reminds covered entities that they should already have in place, and be familiar with applying, minimum necessary policies and procedures that limit the PHI disclosed to a health plan to the amount reasonably necessary to achieve the purpose of the disclosure. Therefore, these procedures and mechanisms should

Important Limitation on an Individual's Right to a Required Restriction: If an individual has a required restriction in place, but does not pay out-of-pocket for follow-up care and the provider needs to include the restricted PHI in order to have the follow-up care deemed medically necessary or appropriate (and therefore paid for by the health plan), then the provider may disclose the restricted PHI to the health plan (provided that the disclosure is consistent with the provider's minimum necessary policies and procedures). *See* 78 Fed. Reg. at 5630.

---

[94] *See* Section 13405(a) of the HITECH Act.

[95] 78 Fed. Reg. at 5628–30 (to be codified at 45 C.F.R. § 164.522(a)(1)(iv)).

[96] *Id.* at 5628.

[97] *Id.* at 5629.

be employed in this context as well to limit the disclosure of PHI subject to a restriction when, for example, a health plan performs an audit of a covered entity's medical records or otherwise requests disclosures of PHI for the health plan's payment or health care operations purposes.[98]

With respect to downstream providers, such as pharmacies and other providers, HHS encourages health care providers to counsel their patients on the patients' obligations to request restrictions from other providers and pay out-of-pocket for follow-up care. For prescribed medication, the prescribing provider will likely need to provide the patient with a paper prescription to allow the patient an opportunity to request a restriction and pay for the prescription before the pharmacy has submitted a bill to the health plan, which generally occurs automatically when an e-prescribing tool is used. Providers should also counsel patients where unbundling of services is not possible or state law prohibits in-network providers from accepting out-of-pocket payments; in such cases, the patient must pay for the entire bundled service or use an out-of-network provider to ensure the PHI is not disclosed to the patient's health plan.[99]

c. Payment in Full

While covered entities are not required to abide by a required restriction if an individual's payment is dishonored, HHS expects that providers will make a "reasonable effort" to contact the individual and obtain payment prior to billing a health plan. HHS does not prescribe what efforts are "reasonable," but instead defers to the provider's policies and the individual circumstances. Providers may choose, however, to require payment in full at the time of the request for a required restriction to avoid payment issues altogether. Therefore, it will be important for covered health care providers to outline clearly in their policies and procedures the "reasonably efforts" the provider will take in such circumstances or if the provider requires payment in full at the time of the request.[100]

2. Right to Access PHI

Expanding on HITECH's requirement to provide individuals with an *electronic* copy of PHI maintained in an *electronic health record* (EHR) system, the Final Rule provides that an individual has a right to obtain an electronic copy of PHI that is maintained in *any electronic system*.[101] Additionally, with regard to PHI maintained in hard copy or electronic designated record sets, HHS limits the time in which covered entities must act on a request, clarifies the reasonable, cost-based fee that a covered entity may charge for providing access to PHI, and sets forth new requirements for an individual's request to provide access and copies directly to third parties.

Under the Existing Privacy Rule, covered entities must provide individuals with access to their PHI that is maintained in a designated record set (hard copy or electronic) in the form or format requested by the individual, if readily producible in such form or format; or, if not, in a *readable hard copy form* or such other form or format as agreed to by the covered entity and the individual. *See* 45 C.F.R. § 164.524.

[98] *Id.* at 5628.

[99] *Id.* at 5629–30.

[100] *Id.*

[101] *See* Section 13405(e) of the HITECH Act; 78 Fed. Reg. at 5631 (to be codified at 45 C.F.R. § 164.524(c)(2)(ii)).

a. Right to Access PHI in an Electronic Form and Format

Under the Final Rule, with respect to PHI maintained in electronic designated record sets, covered entities are now required to provide individuals with access to such PHI 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.

Importantly, HHS acknowledges that the "readable electronic form" will vary by system and does not require covered entities to purchase new software or systems to accommodate a request for a specific electronic form that is not readily producible by the covered entity. However, covered entities must still provide individuals with some kind of readable electronic form and HHS anticipates that some covered entities may need to update legacy or other systems to meet this basic requirement. HHS interprets "readable electronic form" to mean a "digital information stored in a standard format enabling the information to be processed and analyzed by computer," such as MS Word or Excel, text, HTML or text-based PDF.[102]

If an individual requests an electronic form that the covered entity cannot produce, the covered entity must offer other electronic formats that are available of its systems. Only in the event that an agreement cannot be reached between the individual and the covered with regard to an electronic format, the covered entity may provide the individual with a readable hard copy form (as is currently permissible under the existing Privacy Rule with respect to PHI maintained in either hard copy or electronic designated record sets).[103]

b. Covered Entity's Time to Provide Access to PHI

Although not required by the HITECH Act, HHS removes the additional 30 days provided to covered entities to either (1) deny a request or (2) grant and provide access to individuals with regard to PHI that is not maintained or accessible to the covered entity on-site. Under the existing Privacy Rule, covered entities had up to 90 days to respond to an individual's request for PHI maintained off-site.[104] Now, covered entities must take the required action within 60 days regardless of whether the PHI is maintained on- or off-site.[105]

Timely Response under Existing Privacy Rule: Up to 90 Days

- PHI maintained *on-site*:
  - 30 days to take action
  - One 30-day extension
- PHI maintained *off-site*:
  - 60 days to take action
  - One 30-day extension

Timely Response under Final Rule: Up to 60 Days

- PHI maintained *on- or off-site*:
  - 30 days to take action
  - One 30-day extension

c. Fees

Under the existing Privacy Rule, covered entities may charge a reasonable, cost-based fee for providing individuals with access to their PHI. The Final Rule clarifies that such a fee may include labor costs for copying PHI, but may not include labor costs for actually retrieving (or locating) the PHI. In particular, labor costs for copying may include technical staff time spent to create and copy the electronic file, such as compiling, extracting, scanning and burning PHI to media, and distributing the media. Additionally, if, for example, an individual

---

[102] 78 Fed. Reg. at 5631.

[103] *Id.* at 5633.

[104] *See* 45 C.F.R. § 164.524(b)(2)(ii).

[105] 78 Fed. Reg. at 5637.

requests that the covered entity save PHI to a compact disc (CD) and then mail the CD to the individual, the covered entity may charge for the cost of supplies for creating, and the postage for transmitting, the CD.[106]

d. Requests to Provide Access to Third Parties

The Final Rule provides that if requested by the individual, covered entities must transmit a copy of PHI directly to a third party designated by the individual. In such circumstances, the individual's request *must* be in writing, signed by the individual, and clearly identify the designated third party and where to send the copy of the PHI. While covered entities may rely on the information provided by the individual in the written request, covered entities must also implement reasonable policies and procedures under Section 164.514(h) to verify the identity of the individual making the request, as well as implement reasonable safeguards under Section 164.530(c) to protect the PHI that is used or disclosed. Such safeguards include, for example, ensuring that the covered entity correctly enters in the e-mail address of the third party into its system.[107]

K. Decedents

1. 50 Year Period of Protection for Decedent Information

The Final Rule adopts the modification that a covered entity must protect an individual's health information for 50 years following the death of the individual. HHS notes that the majority of public commenters favored this 50-year limitation, though some commenters opposed this limit due to continued privacy interests of the decedent and living relatives. Importantly, in response to commenters' concerns regarding particularly sensitive PHI, HHS reminds covered entities that the 50-year limitation does not interfere with or override state or other laws that provide greater protections, or the professional responsibilities of mental health or other providers. HHS also cautions that the Privacy Rule does not include medical record retention requirements; therefore, this 50-year limitation is a period of protection—not a record retention requirement.[108]

2. Disclosures About a Decedent to Family Members and Others Involved In Care

The Final Rule adopts the proposal to permit covered entities to disclose a decedent's PHI to certain individuals listed in Section 164.510(b)(1), including family members and others who were involved in either the care or payment for care of the decedent before the decedent's death; however, a covered entity may not disclose such PHI to the named individuals if "doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity."[109]

While the language in this new standard is vague, the preamble does offer some guidance. In response to commenters who questioned what it means for a person to have been "involved with care" before a decedent's death, HHS indicates that covered entities should have "reasonable assurance the individual prior to death was involved in the individual's care or payment for care." Additionally, the prohibition against a covered entity disclosing PHI if "doing so is inconsistent with any prior expressed preference . . . that is known to the covered entity" seems to place a high burden on a covered entity. Unfortunately, the Final Rules does not provide

---

[106] *Id.* at 5635–36 (to be codified at 45 C.F.R. § 164.524(c)(4)).

[107] *Id.* at 5634–35 (to be codified at 45 C.F.R. § 164.524(c)(3)(ii)).

[108] *Id.* at 5614 (to be codified at 45 C.F.R. § 164.502(f)).

[109] *Id.* at 5615 (to be codified at 45 C.F.R. § 164.510(b)(5)).

guidance as to what reaches the threshold of "prior expressed preference" and what it means for a covered entity to have knowledge of that preference.[110]

The preamble to the Final Rule also makes clear that the disclosures are permissive and not required and underscores the Privacy Rule's limitation on such disclosures "to the protected health information relevant to the family member or other person's involvement in the individual's health care or payment for health care." In providing the example of a covered entity providing billing information to a decedent's family member who is wrapping up the decedent's estate, the preamble indicates that "the provider generally should not share information about past, unrelated medical problems."[111]

* * *

With the Final Rule's delayed general compliance date allowing for covered entities and business associates to spend some time digesting the new and varied implications to HIPAA compliance, now is the time to review business relationships involving PHI, as well as the associated HIPAA policies and procedures.

[110] *Id.* at 5615.

[111] *Id.* at 5615–16.