COVINGTON

COVINGTON & BURLING LLP

ADVISORY | Health Care

February 7, 2013

HHS ISSUES LONG-AWAITED FINAL HITECH OMNIBUS RULE

On January 25, 2013, the U.S. Department of Health and Human Services (HHS) published in the *Federal Register* its long-awaited final omnibus rule (available here) modifying the privacy, security, enforcement, and breach notification regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[1] The omnibus rule is comprised of the following four rules:

1. Final modifications to the HIPAA regulations mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, and certain other modifications to improve the HIPAA rules;
2. Final rule adopting changes to the HIPAA Enforcement Rule;
3. Final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act; and
4. Final rule modifying the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act of 2008 (GINA).

The rule is effective March 26, 2013, but covered entities and business associates have until September 23, 2013, to comply with most new requirements.[2]

This advisory describes key aspects of the final omnibus rule, including changes affecting business associates and their subcontractors; business associate agreements; breach notification; research; marketing; sale of protected health information (PHI); HIPAA notices of privacy practices; individual rights; enforcement; and genetic information. The material in this advisory is a compilation of analyses that have already been published on our blog, InsidePrivacy (available here). This advisory is intended as a service to those who are interested in having a comprehensive summary, as well as citations to the final omnibus rule.

BUSINESS ASSOCIATES AND THEIR SUBCONTRACTORS

The final HITECH omnibus rule includes a number of changes that will significantly affect business associates and their subcontractors. Business associates are now directly subject to various aspects of the HIPAA Privacy, Security, and Breach Notification Rules. Furthermore, liability now extends much further down the chain, as the new rule also applies these requirements to subcontractors of business associates.

Definition of "Business Associate"

The final rule revises the definition of "business associate" to include an entity that "creates, receives, maintains, or transmits" PHI.[3] HHS explained that this new definition will include entities that maintain or store PHI, even if they do not actually view the PHI.[4] As a result, organizations such as Health Information Organizations, E-prescribing Gateways, Personal Health Record (PHR) vendors,

---

[1] 78 Fed. Reg. 5,566 (Jan. 25, 2013).
[2] *Id.* at 5,569-70.
[3] *Id.* at 5,572.
[4] *Id.*

and others that provide data transmission services involving PHI will now be considered business associates.[5]

Direct Liability under the Security Rule

The final rule expressly subjects business associates to the administrative, physical, and technical safeguard requirements of the Security Rule.[6] HHS commented that, because business associates previously had to agree in their business associate agreements with covered entities to appropriately protect and safeguard PHI, business associates and subcontractors "should already have in place" security practices that are compliant with the rule, but recognized that many business associates will not have engaged in the "formal administrative safeguards" required by the rule.[7]

Direct Liability under the Privacy Rule

The final regulations modify the Privacy Rule to extend direct liability for disclosures of PHI by business associates.[8] However, the rule does not subject business associates to liability for all aspects of the Privacy Rule. Business associates are liable for:

- uses or disclosures of PHI in a manner not in accord with the business associate agreement or the Privacy Rule;
- failure to disclose PHI when required by HHS for an investigation and/or determination of the business associate's compliance with HIPAA;
- failure to disclose PHI to the covered entity, an individual (to whom the information pertains), or the individual's designee with respect to an individual's request for an electronic copy of the information;
- failure to make reasonable efforts to limit PHI uses, disclosures, and requests to the minimum necessary amount; and
- failure to enter into a business associate agreement with a subcontractor that creates or receives PHI on their behalf.[9]

Business associates may use or disclose PHI only as permitted or required by their business associate agreements or as required by law. If a permitted disclosure is not specified in a business associate agreement or other similar contract, the disclosure is not permitted—even if it would otherwise be permissible by a covered entity.

Direct Liability under the Breach Notification Rule

The HITECH Act requires a business associate to notify the covered entity when it discovers a breach of unsecured PHI. The final rule implements this statutory requirement. The rule requires the business associate to provide notice of the breach to the covered entity "without unreasonable delay and in no case later than 60 days" following discovery of a breach.[10]

If the business associate is acting as an agent of the covered entity, then the business associate's discovery will be imputed to the covered entity.[11] A covered entity is required to notify HHS of breaches within a certain allotted time measured by when its agent (the business associate) discovered the breach, not when the covered entity became aware. HHS noted that it will use federal common law of agency to determine whether the business associate is acting as an agent.[12]

---

[5] *Id.*
[6] *Id.* at 5,589.
[7] *Id.*
[8] *Id.* at 5,591.
[9] *Id.*
[10] *Id.* at 5,651.
[11] *Id.* at 5,655.
[12] *Id.*

Thus, covered entities should ensure that their business associate contracts adequately address how and when a business associate will notify the covered entity of a suspected breach.

Subcontractors

One of the most significant changes in the rule is the extension of HIPAA requirements applicable to business associates to subcontractors. Under the final rule, a subcontractor is an entity that "creates, receives, maintains, or transmits" PHI on behalf of a business associate. [13] A subcontractor must enter into a business associate agreement with the primary business associate.[14]

The final rule requires a business associate to obtain assurances from its subcontractors that they will appropriately safeguard PHI. This provision "mirrors" the one requiring covered entities to obtain similar assurances from business associates. Similarly, a business associate that is aware of noncompliance by its subcontractor must respond in the same manner as a covered entity that is aware of noncompliance by its business associate.[15]

Minimum Necessary Standard

The final rule requires that, when business associates use, disclose, or request PHI from another covered entity, they limit PHI to that minimally necessary to accomplish the purpose of the use, disclosure, or request.[16] Failure to abide by the minimum necessary requirement is a violation of the Privacy Rule. HHS noted that how business associates will apply this standard will "vary based on the circumstances."[17] HHS stated that it will issue future guidance on the specific application of the minimum necessary standard to business associates.[18]

BUSINESS ASSOCIATE AGREEMENTS

The final rule addresses several changes to business associate agreements as a result of the new obligations imposed upon business associates by HITECH. HHS also published sample business associate agreement provisions that reflect these new requirements, which are available here.

New Obligations for Business Associates

A revised section 45 C.F.R § 164.504(e) expands the list of specific requirements for business associate agreements to require that business associates:

- comply with the Security Rule with regard to electronic PHI;
- report breaches of unsecured PHI to covered entities;
- comply with the requirements of the Privacy Rule applicable to covered entities when carrying out their obligations; and
- ensure that any subcontractors that create or receive PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate.

In the event that the covered entity is aware that actions of the business associate constitute a material breach or violation of the business associate agreement, the revised rule removes the requirement that covered entities report to the Secretary when termination of a business associate agreement is not feasible.[19]

---

[13] *Id.* at 5,688 (Final 45 C.F.R. § 160.103).
[14] *Id.* at 5,698 (Final 45 C.F.R. § 160.504(e)(5)).
[15] *Id.* at 5,600.
[16] *Id.* at 5,559.
[17] *Id.*
[18] *Id.*
[19] *Id.* at 5,600-01.

Subcontractors

The final rule allows a business associate to disclose PHI to a business associate that is a subcontractor, as long as the business associate enters into an appropriate business associate agreement with its subcontractor. [20] The covered entity is not required to enter into an agreement with a subcontractor; rather, the responsibility is on the business associate.[21] The business associate is therefore contractually liable to the covered entity for any business associate operations that it outsources to a contractor. [22] A subcontractor that enters into a business associate agreement with the primary business associate will be directly liable under HIPAA.

Furthermore, the final rule clarifies that a subcontractor may not use PHI in any way that is not permitted by the business associate agreement between the primary business associate and the covered entity. HHS explained that each agreement in the "business associate chain must be as stringent or more stringent" than the agreements above it in the chain.[23]

The final rule also adds a new obligation on business associates with regard to their subcontractors that "mirrors" the obligations covered entities have for business associates. If a primary business associate is aware that its subcontractor is out of compliance with its business associate agreement, the primary business associate is required to take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, then the primary business associate must terminate the arrangement, if feasible.[24]

Obligations of Business Associates Under Agreements

Although the HITECH Act and the final HITECH omnibus rule impose direct liability on a business associate for failure to abide by certain HIPAA requirements, the business associate still retains contractual liability to the covered entity for failure to comply with the business associate agreement. The final rule adds a provision that clarifies that when a covered entity delegates its responsibility to a business associate to carry out certain responsibilities, the business associate is contractually obligated to comply with the requirements of the Privacy Rule in the same manner as the covered entity.[25]

Timeline for Compliance

HHS has allowed additional time for covered entities and business associates to revise their agreements in accordance with the new requirements. For agreements in effect as of January 25, 2013, parties have until September 22, 2014, to modify their business associate agreements, unless the parties renew or modify their current contracts between March 26, 2013 (date the final rules take effect) and September 23, 2013 (deadline for compliance with other provisions of the final rule).[26] In these circumstances, the business associate agreement must be in compliance with the new rules by September 23, 2013.[27]

HIPAA BREACH NOTIFICATION RULE

The HITECH omnibus rule establishes a new standard for determining whether an unauthorized use or disclosure of unsecured PHI is a "breach" requiring notification.[28] Under the current Breach Notification Rule, covered entities are required to notify individuals of a breach involving their

---

[20] *Id.* at 5,599.
[21] *Id.*
[22] *Id.*
[23] *Id.* at 5,601.
[24] *Id.* at 5,600.
[25] *Id.* at 5,601.
[26] 45 C.F.R. § 164.532(e).
[27] *Id.*
[28] 78 Fed. Reg. at 5,695.

unsecured PHI, and business associates have a corresponding obligation to notify covered entities.[29] The current rule states that an unauthorized use or disclosure of PHI is a "breach" if it poses a significant risk of financial, reputational, or other harm to the individuals affected.[30]

The omnibus rule replaces the "risk of harm" test with a default presumption that any acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule is a breach unless the covered entity or business associate "demonstrates that there is a low probability that the [PHI] has been compromised based on a risk assessment."[31] HHS stated that the omnibus rule establishes a presumption that uses or disclosures of PHI in violation of the Privacy Rule are "breaches" because HHS believes that many covered entities and business associates have construed the existing "risk of harm" standard as setting a higher bar than HHS intended.[32] Covered entities and business associates now have the burden of proving that there is a "low probability" that PHI has been compromised through a risk assessment that accounts for at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.[33]

All of these factors must be considered in combination.[34] If a covered entity or business associate determines that an unauthorized use or disclosure of PHI is not a breach, it will need to maintain documentation sufficient to overcome the presumption that PHI was compromised.[35] HHS suggests that these risk assessments allow for a more "objective" evaluation than the current "risk of harm" standard,[36] and plans to provide further guidance on risk assessments that addresses "frequently occurring scenarios."[37]

The omnibus rule also removes a provision from the current rule's definition of a "breach," which says that PHI is not compromised if a use or disclosure in violation of the Privacy Rule involves a limited data set that does not contain dates of birth or zip codes.[38] While unauthorized uses or disclosures of a limited data set are now subject to the same presumption of breach, HHS suggested that, in most instances, the risk assessment would result in a finding of a low probability that the PHI had been compromised and, thus, no breach had occurred.[39] The omnibus rule also revises the breach notification provision related to notifying HHS. Covered entities are required to notify HHS immediately of any breach affecting more than 500 individuals.[40] In addition, covered entities must annually submit a log to HHS of each breach affecting fewer than 500 individuals.[41] The omnibus rule modifies the rule to clarify that covered entities must report breaches affecting fewer than 500 individuals to HHS "not later than 60 days after the end of the calendar year in which the breaches were 'discovered,' not in which the breaches 'occurred.'"[42] Thus, if a breach affecting 400

---

[29] *See* 45 C.F.R. Part 164, Subpart D.
[30] 45 C.F.R. § 164.402.
[31] 78 Fed. Reg. at 5,695.
[32] *Id.* at 5,641.
[33] *Id.* at 5,695.
[34] *Id.* at 5,643.
[35] *Id.* at 5,641.
[36] *Id.* at 5,641-42.
[37] *Id.* at 5,643.
[38] *Id.* at 5,644.
[39] *Id.*
[40] 45 C.F.R. § 164.408(b).
[41] 45 C.F.R. § 164.408(c).
[42] 78 Fed. Reg. at 5,654.

individuals were to occur in December 2013 and were to be discovered in January 2014, the covered entity would not be required to report the breach to HHS until the first 60 days of 2015.

The omnibus rule otherwise retained the existing Breach Notification Rule with only stylistic and non-substantive modifications.

HIPAA REQUIREMENTS FOR RESEARCH AUTHORIZATIONS

The final HITECH omnibus rule contains major changes to the HIPAA requirements for research authorizations. Specifically, as described below, HHS has loosened the current restrictions on "compound authorizations" for research purposes, and is now interpreting the HIPAA Privacy Rule to allow authorizations for future research.[43] These changes could have a tremendous impact on the manner in which informed consent for clinical trials is documented in the United States and on the availability of clinical trial data for future research.

Compound Authorizations

The HIPAA Privacy Rule generally prohibits "compound authorizations," which are authorizations that are combined with any other legal permission.[44] An exception allows the combining of an authorization for a research study with written permission for the same study, usually found in an informed consent form.[45] But under the current rules, this exception is not available if one authorization conditions treatment, payment, enrollment in a health plan, or eligibility for benefits on the individual providing an authorization (conditioned authorization) and the other authorization does not contain such conditions (unconditioned authorization).[46] This prevents a covered entity from, for example, using a single authorization for a research study that covers both treatment as part of a clinical study and tissue banking of specimens for future research. Many groups have informed HHS that this lack of integration is inconsistent with the Common Rule (45 C.F.R. Part 46) and creates unnecessary documentation burdens.[47]

In the final HITECH omnibus rule, HHS adopted its proposal to amend the authorization requirements to allow a covered entity to combine conditioned and unconditioned authorizations for research, provided the authorization:

- clearly differentiates between the conditioned and unconditioned research components; and
- provides the individual with an opportunity to opt in to the unconditioned research activities.[48]

The revised 45 C.F.R. § 164.508(a)(3)(i) also specifically provides that an authorization for a research study may be combined with "an authorization for the creation or maintenance of a research database or repository."[49]

Although the preamble sets forth a number of possible methods that would satisfy the differentiation and opt-in requirements, HHS emphasized that covered entities and researchers have flexibility to determine the best approach for meeting the requirements.[50]

Authorizations for Future Research

In addition to revising the authorization requirements, HHS, in the preamble to the final rule, reversed its prior interpretation that a research authorization must be study specific and therefore cannot include an authorization for future research.[51]

---

[43] *Id.* at 5,609-13.
[44] 45 C.F.R. § 164.508(b)(3).
[45] *Id.*
[46] *Id.* § 164.508(b)(4).
[47] 78 Fed. Reg. at 5,609.
[48] *Id.* at 5,610.
[49] *Id.* at 5,699.
[50] *Id.* at 5,610.

The prior policy had been based on a concern that the lack of specific information about future research would make it impossible for subjects to make an informed decision about the use of their PHI for that future research.[52] However, HHS noted that it had heard from many researchers and other groups that this interpretation encumbers secondary research and diverges from current practice under the Common Rule.[53]

In the preamble to the final rule, HHS stated that it was modifying its prior interpretation to allow authorizations for future research.[54] Under this modification, HHS interprets the requirement in 45 C.F.R. § 164.508(c)(1)(iv) that the authorization must include a description of each purpose of the use or disclosure to mean that the authorization for future research must "adequately describe such purposes such that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for such future research."[55] HHS stated that this approach gives covered entities, researchers, and Institutional Review Boards (IRBs) flexibility in determining how best to describe a future research purpose, and that it consulted with the Food and Drug Administration (FDA) and the Office for Human Research Protections on this approach to ensure consistency with the HHS and FDA human research protections.[56]

Interestingly, HHS also stated that covered entities and researchers may rely on an IRB-approved consent obtained prior to the effective date of the final rule that reasonably informs individuals about future research, as long as the informed consent was combined with a HIPAA authorization (even if the authorization was specific to the original study or creation and maintenance of a repository).[57]

HIPAA MARKETING REQUIREMENTS

The final HITECH omnibus rule significantly tightens the HIPAA marketing restrictions. As described below, HHS has modified the proposed approach to require authorization for almost all treatment and health care operations communications where the covered entity receives, from a third party, financial remuneration for making the communication. This change will have major implications for the design of medical messaging programs.

Background

The HIPAA Privacy Rule generally requires that a covered entity obtain prior written authorization from an individual before using that individual's PHI for marketing purposes.[58] Prior to the HITECH Act, certain communications, including those related to treatment and care coordination, were excluded from the definition of marketing.[59] But under the HITECH Act, if a covered entity or business associate receives direct or indirect payment in exchange for making certain communications (including those related to treatment and care coordination), the covered entity generally must obtain prior authorization–unless the communication qualifies for a limited exception for communications about currently prescribe drugs or biologics where the payment received is reasonable in amount.[60]

---

[51] *Id.* at 5,611-13.
[52] *Id.* at 5,611-12.
[53] *Id.* at 5,612. We discussed these concerns, and HHS's proposed options to address this issue, in a blog post available here.
[54] *Id.* at 5,612.
[55] *Id.*
[56] *Id.* at 5,613.
[57] *Id.*
[58] 45 C.F.R. § 164.508(a)(3).
[59] *Id.* § 164.501.
[60] HITECH Act § 13406(a).

To implement the HITECH Act marketing provisions, HHS proposed to:

- exclude from the definition of "marketing" certain health care operations communications, except where the covered entity receives financial remuneration in exchange for the communication;
- exclude from the definition of "marketing" communications about refill reminders or otherwise about a drug or biologic that is currently being prescribed for the individual, as long as any financial remuneration received for making the communication is reasonably related to the covered entity's cost of making the communication; and
- exclude from the definition of "marketing" treatment communications about health-related products or services by a health care provider to an individual, provided that if the communications are in writing and the covered entity receives financial remuneration in exchange for making them, certain notice and opt-out conditions are met.[61]

Final Marketing Requirements

In the final HITECH omnibus rule, HHS modified the proposal to require authorization for all subsidized treatment and health care operations communications, with a narrow exception for communications about currently prescribed drugs.[62] The final rule also retains the current exceptions to the authorization requirement for face-to-face communications and promotional gifts of nominal value.[63]

HHS explained in the preamble that it decided to adopt this policy, instead of the proposed approach, because it concluded that the difficulty of distinguishing between treatment communications and health care operations communications could place covered entities at risk of violating the HIPAA marketing requirements.[64]

Financial Remuneration. The final omnibus rule adopts the proposed definition of "financial remuneration," which is "direct or indirect payment from or on behalf of a third party whose product or service is being described."[65] The term does not include payment for treatment of an individual or non-financial or in-kind benefits.[66] HHS also clarified in the preamble that, where a business associate or subcontractor receives financial remuneration in exchange for making a marketing communication, that communication also requires prior authorization from the individual.[67]

Authorizations for Marketing. Under the revised 45 C.F.R. § 164.508(a)(3), a covered entity must obtain a valid authorization from the individual before using or disclosing PHI for marketing communications that involve financial remuneration.[68] The authorization must disclose the fact that the covered entity (or business associate or subcontractor, if applicable) is receiving remuneration from a third party.[69]

Authorization Exceptions. HHS specifically stated in the preamble that the final rule does not modify the existing exceptions to the authorization requirement for face-to-face marketing communications or promotional gifts of nominal value provided by the covered entity.[70] HHS offered the following example: Authorization is not required if a health care provider, in a face-to-face conversation with an individual, verbally or by handing a written pamphlet to the individual, recommends "that the

---

[61] 78 Fed. Reg. at 5,592-93. For more on HHS's proposed approach to marketing, see our blog posts here and here.
[62] *Id.* at 5,595.
[63] *Id.* at 5,596.
[64] *Id.* at 5,595.
[65] *Id.*
[66] *Id.* at 5,696.
[67] *Id.* at 5,595.
[68] *Id.* at 5,699.
[69] *Id.*
[70] *Id.* at 5,596.

individual take a specific alternative medication, even if the provider is otherwise paid by a third party to make such communications."[71]

Communications About Currently Prescribed Drugs. The final omnibus rule adopts the proposed exception for a communication made to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, provided that any financial remuneration received by the covered entity for making the communication is reasonably related to the covered entity's cost of making the communication.[72]

HHS clarified in the preamble that this exception includes communications regarding:

- the generic equivalent of a drug being prescribed to an individual
- adherence communications encouraging individuals to take their prescribed medications
- all aspects of a drug delivery system (including, for example, an insulin pump) for a self-administered drug or biologic that has been prescribed for an individual.[73]

HHS also stated that it intends to issue future guidance on other communications that fall within this exception.[74]

With respect to the limit on financial remuneration, HHS clarified that "permissible costs for which a covered entity may receive remuneration under this exception are those which cover only the costs of labor, supplies, and postage to make the communication."[75] This does not include any profit or payment for other costs.[76]

Other Exempt Communications. In addition to the exceptions described above, HHS clarified in the preamble that the following communications are exempt from the marketing requirements:

- communications promoting health in general, which do not promote a product or service from a particular provider
- communications about government and government-sponsored programs, such as Medicare, Medicaid, or the State Children's Health Insurance Program.[77]

SALE OF PROTECTED HEALTH INFORMATION

The final rule implements Section 13405(d) of the HITECH Act, which generally prohibits a covered entity or a business associate from engaging in a "sale" of an individual's PHI without authorization.

Definition of Sale of PHI

At the request of commenters, HHS amended its proposal to provide a definition of "sale of PHI." Section 164.502(a)(5)(ii)(B)(1) defines "sale of PHI" to mean a disclosure of PHI when 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."[78] HHS expressly refused to limit this definition to instances where there is a transfer of ownership of PHI.[79] Furthermore, HHS included a broad interpretation of "remuneration." In contrast to the marketing provision where remuneration must

---

[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] *Id.* at 5,597.
[76] *Id.*
[77] *Id.*
[78] 78 Fed. Reg. at 5,696-97; 45 C.F.R. § 164.502(a)(5)(ii)(B)(1).
[79] *Id.* at 5,606.

be financial, HHS will consider nonfinancial benefits received in exchange for PHI as falling within the scope of the rule.[80]

HHS noted, however, that payments a covered entity may receive in the form of grants, contracts, or other arrangements to perform programs or activities using PHI (i.e., a research study) will not be considered sale of PHI because "any provision of PHI to the payer is a byproduct of the service being provided."[81] Rather, a sale of PHI occurs when the covered entity or business associate is being compensated "primarily" for supplying PHI.[82]

Exceptions

The final rule includes several exceptions under which covered entities and business associates may conduct a "sale of PHI," and receive financial or non-financial remuneration in exchange for providing PHI, without having to obtain authorization:

- For public health purposes as enumerated in the rule;
- For research purposes, but only when remuneration is a "reasonable cost-based fee to cover the cost to prepare and transmit" the PHI;
- For purposes of treatment and payment as allowed in the rule;
- For the sale, transfer, merger, or consolidation of all or part of a covered entity and for related due diligence;
- To or by a business associate for activities the business associate undertakes on behalf of the covered entity (including a subcontractor);
- To the individual when requested or in connection with an accounting of disclosures if the fees are in accordance with the Privacy Rule;[83]
- When required by law;
- For any purpose permitted by and in accordance with the Privacy Rule, as long as the remuneration is a "reasonable cost-based fee to cover the cost to prepare and transmit" the PHI.[84]

Redisclosures

HHS noted that "it is expected to be the usual case" that a separate, additional authorization would be required before the recipient may redisclose an individual's PHI for remuneration. However, HHS also stated that "it may be possible that redisclosures of information for remuneration by a recipient covered entity or business associate do not require an additional authorization, provided it is sufficiently clear to the individual in the original authorization that the recipient covered entity or business associate will further disclose the individual's PHI in exchange for remuneration."[85]

Prior Authorizations Before Compliance Date

Several commentators expressed concern that this new requirement could endanger research studies based on a prior permission under the Privacy Rule that does not give the covered entity or business associate the authorization to "sell" PHI for remuneration. HHS clarified that a covered entity may continue to rely on a prior authorization obtained before the compliance date (September

[80] *Id.* at 5,607.
[81] *Id.* at 5,606.
[82] *Id.*
[83] The covered entity may impose only a reasonable, cost-based fee that includes only postage and the cost of labor and supplies for copying and preparing an explanation of the summary of PHI. 45 C.F.R. § 164.524(c)(4).
[84] 45 C.F.R. § 164.502(a)(5)(ii).
[85] 78 Fed. Reg. at 5,608.

23, 2013) "even if remuneration is involved."[86] This grace period is available for all any permissible disclosure under the Privacy Rule, not just for research purposes.[87]

HIPAA NOTICES OF PRIVACY PRACTICES

The final HITECH omnibus rule requires covered entities to add several new provisions to the Notice of Privacy Practices (NPP) that they distribute to patients and beneficiaries.[88] Generally, an NPP describes how the covered entity may use and disclose PHI, an individual's rights with respect to PHI (e.g., the right to access PHI and request restrictions on uses and disclosures), and the covered entity's legal duties with respect to PHI (e.g., the duty to abide by the terms of the NPP).

- *Uses and Disclosures Requiring Authorization*. The omnibus rule requires a covered entity to include a separate statement informing individuals that certain uses and disclosures require authorization.[89] Specifically, NPPs must state that the following require an individual's prior authorization: (1) most uses and disclosures of psychotherapy notes (if the covered entity maintains psychotherapy notes); (2) uses and disclosures of PHI for marketing purposes; and (3) disclosures of PHI that constitute a "sale."[90]
- *Opting Out of Fundraising Communications*. If a covered entity contacts individuals for fundraising purposes, its NPP must notify individuals that they have a right to opt out of such communications, although the NPP does not need to describe the mechanism for opting out of receiving such communications.[91] Each fundraising communication will specify the opt out option(s) available.[92]
- *Restricting Certain Disclosures*. A health care provider's NPP must inform individuals of their right to restrict certain disclosures of PHI to health plans when the individual has paid in full for a health care item or service.[93]
- *Breach Notification*. The NPP must inform individuals of their right to receive a notification in the event of a breach of their unsecured PHI.[94] In the preamble, HHS explained that a "simple statement . . . that an individual has a right to or will receive" a breach notification in appropriate circumstances "will suffice for purposes of this requirement."[95] No further description is required.

HHS stated that the modifications required above are "material changes" to a covered entity's NPP.[96] As a result, covered entities must notify individuals of these material changes in accordance with the Privacy Rule. The omnibus rule also revises and clarifies how covered entities are required to notify individuals of material changes:

- *Health Plans*. If a health plans posts an NPP on its website, it must post the revised NPP with the material change on its website by the effective date of the material change, and also "provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals covered then by the plan."[97] If the health plan does not have a website where it posts its NPP, it must "provide the revised notice, or information about the material change and how to obtain the revised notice, to individuals then

[86] *Id.*
[87] *Id.*
[88] *Id.* at 5,701.
[89] *Id.* at 5,624.
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] *Id.* at 5,625.
[97] *Id.*

covered by the plan within 60 days" of the material change.[98] In the preamble, HHS also suggested that health plans should provide beneficiaries with "both paper- and web-based notices."[99]

- *Health Care Providers*. The omnibus rule does not change the requirements for health care providers to inform patients of material changes to their NPPs.[100] However, the preamble does discuss how health care providers should distribute and display their NPPs.[101] For example, HHS explained that health care providers may post a summary of their NPP "in a clear and prominent location at the delivery site" if the full NPP is "immediately available" to patients (*i.e.*, on a table next to the posted summary) and there is no additional burden to acquire the full NPP.[102] Requiring patients to ask a receptionist for the full NPP would be considered an unacceptable burden.[103]

CHANGES TO INDIVIDUAL RIGHTS

The final HITECH omnibus rule implements provisions in the HITECH Act pertaining to two individual rights: an individual's right to request a restriction on the disclosure of his or her PHI and an individual's right to access his or her PHI.[104]

Right to Restrict Uses and Disclosures of PHI

The current Privacy Rule grants individuals the right to request restrictions on the use or disclosure of their PHI, but covered entities are not required to agree to such restrictions.[105] The HITECH Act strengthens the right to request restrictions on disclosures by requiring covered entities to accept a restriction on disclosing PHI to a health plan where the disclosure is for payment or health care operations purposes and the PHI "pertains solely to a health care item or service for which the health care provider involved as been paid out of pocket."[106]

The omnibus rule amends the Privacy Rule to account for this provision.[107] The restriction applies only where the service or item has been paid in full out of pocket; it does not apply to follow-up visits if they are not paid for in full out of pocket.[108]

The preamble discussed more specific applications of the rule and examines various complicating issues, including bundled services, providers participating in HMOs, and dishonored payments.[109]

Right of Access to PHI

The omnibus rule also revises the section of the Privacy Rule pertaining to an individual's right to access his or her PHI that is maintained in a designated record set.[110] The HITECH Act establishes that individuals have a right to obtain a copy of their PHI in electronic format where it is maintained in an Electronic Health Record (EHR).[111] In the preamble, HHS expressed concern that applying these requirements only to EHRs and not accounting for other PHI stored electronically could lead to confusion.[112] Consequently, under the final omnibus rule, individuals have a right to obtain an

[98] *Id.*
[99] *Id.*
[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *Id.* at 5,701-02.
[105] 45 C.F.R. § 164.522.
[106] HITECH Act § 13405(a).
[107] 78 Fed. Reg. at 5,701.
[108] *Id.*
[109] *Id.* at 5,629-30.
[110] *Id.* at 5,701-02.
[111] HITECH Act § 13405(e).
[112] 78 Fed. Reg. at 5,702.

electronic copy of their PHI if the PHI is "maintained in one or more designated record sets electronically."[113]

- *File Format*. The omnibus rule establishes that, if electronic PHI is not readily producible in the requested format, the covered entity must provide a copy of the PHI in another "readable electronic form" (e.g., a PDF) rather than a hard copy.[114]
- *Third Parties*. The final rule requires covered entities to transmit a copy of PHI to another person if requested by the individual, regardless of whether the PHI is maintained in an EHR.[115]
- *Fees*. The HITECH Act prohibits covered entities from charging more than their labor costs in responding to a request for a copy of PHI that is maintained in an EHR.[116] The final rule provides that covered entities may charge certain labor and supply costs associated with providing an electronic copy of PHI.
- *Timing*. The final rule provides that covered entities must respond to all requests within 30 days, regardless of where the PHI is stored, unless they are granted the one-time 30-day extension.[117]

HIPAA ENFORCEMENT

The final HITECH omnibus rule adopts a number of modifications to Subparts C and D of Part 160 (HIPAA Enforcement Rule) to implement Section 13410 of the HITECH Act. Most significantly, the rule includes modifications to implement Section 13410(a) of the HITECH Act, which requires HHS to formally investigate a complaint if a preliminary investigation indicates a possible violation due to willful neglect, and to impose a civil money penalty for a violation due to willful neglect.[118]

In addition, the rule:

- Modifies the definition of "reasonable cause" in 45 C.F.R. § 160.401 to clarify the mens rea associated with this category of violations;[119]
- Amends 45 C.F.R. § 160.402(c) to make covered entities and business associates liable for the acts of their business associate agents;[120]
- Retains the revised penalty structure in 45 C.F.R. § 160.404(b) as implemented by the interim final rule;[121] and
- Adopts other proposed modifications and provisions in the interim final rule regarding factors considered in determining the amount of a civil penalty, affirmative defenses, HHS's waiver authority, and calculation of the 30-day cure period for willful neglect violations.[122]

PRIVACY RULES TO PROTECT GENETIC INFORMATION

In addition to finalizing the HIPAA regulations under HITECH, the omnibus rule finalized modifications to the HIPAA Privacy rule required by GINA. GINA prohibits discrimination in employment and health insurance coverage based on a person's genetic information. Specifically, GINA prohibits health plans from using the genetic information of an individual, for example that he or she is predisposed to develop a certain genetic disorder or carries a specific genetic mutation, for underwriting purposes.

---

[113] *Id.*
[114] *Id.*
[115] *Id.*
[116] HITECH Act § 13405(e)(2).
[117] *Id.*
[118] HITECH Act § 13410(a); 78 Fed. Reg. at 5,578.
[119] 78 Fed. Reg. at 5,579.
[120] *Id.* at 5,580.
[121] *Id.* at 5,583.
[122] *Id.* at 5,584-87.

GINA directed HHS to make modifications to the HIPAA Privacy Rule. In October 2009, HHS promulgated proposed rules to:

- Clarify that genetic information is health information for purposes of PHI;
- Prohibit health plans from using or disclosing PHI containing genetic information for underwriting purposes;
- Revise the provisions related to the Notice of Privacy Practices for health plans that perform underwriting; and
- Make technical corrections to update the definition of "health plan."[123]

The structure of the final rules issued by HHS track these proposed rules, while making some modifications to the details of the individual proposals.

Prohibition on Underwriting

Health plans may not use or disclose genetic information for underwriting purposes. This prohibition applies to all plans subject to the HIPAA Privacy Rule, with one exception. In a departure from the proposed rule, the final regulations exempt long-term care (LTC) insurers from this prohibition. However, HHS said that it will continue to look into ways to address privacy concerns raised by the use of genetic information for underwriting by LTC insurers--including through a study by the National Association of Insurance Commissioners (NAIC).[124]

The final rule also makes clear that this prohibition is limited to health plans--a health care provider may use genetic information for treatment.[125]

Definitions

The final regulations include definitions for the following terms:

- "*health information*" is defined to include "genetic information;"[126]
- "*genetic information*" is defined to include any genetic information including an individual or family member but excludes information about age, sex, or non-genetic manifested diseases or disorders;[127]
- "*genetic tests*" means analyses of DNA, RNA, chromosomes, proteins, or metabolites that detects genotypes, mutations, or chromosomal changes;[128]
- "*genetic services*" means genetic tests, counseling, or education -- including the fact that a person received a genetic test, counseling, or education;[129]
- "*family member*" means any dependent or other individual who is a first, second, third, or fourth degree relative;[130]
- "*manifestation or manifested*" means, with respect to a disease or disorder, that an individual could reasonably be diagnosed by a health care professional with appropriate training and expertise in the field involved and the diagnosis is not principally based on genetic information (diseases that are manifested are not subject to the prohibition);[131]

---

[123] *Id.* at 5,659-60.
[124] *Id.* at 5,661.
[125] *Id.* at 5,667.
[126] *Id.* at 5,661.
[127] *Id.* at 5,662.
[128] *Id.*
[129] *Id.* at 5,663.
[130] *Id.*
[131] *Id.* at 5,664.

- the definition of "*health care operations*" is amended to include a reference to the prohibition on using or disclosing genetic information for underwriting purposes.[132]
- the definition of "*payment*" makes clear that health plans may use results of genetic tests for purposes of payment (such as determining eligibility for benefits) as long as these activities do not constitute "underwriting purposes."[133]

Notice of Privacy Practices (NPP)

The final rule requires health plans that perform underwriting to include in their NPPs that they are prohibited from using or disclosing genetic information for this purpose, except with regard to LTC policies. Health plans that have already modified their NPPs to reflect the statutory prohibition in GINA are not required to re-issue their NPPs.[134]

If you have any questions concerning the material discussed in this client alert, please contact the following members of our health care practice group:

Anna Kraus	202.662.5320	akraus@cov.com
Rachel Grunberger	202.662.5033	rgrunberger@cov.com
Shelton Abramson	202.662.5184	sabramson@cov.com
Dena Feldman	202.662.5192	dfeldman@cov.com

---

[132] *Id.* at 5,666.
[133] *Id.*
[134] *Id.* at 5,688.