**HHS issues final omnibus HIPAA/HITECH rule**

* [Foley & Lardner LLP](http://www.lexology.com/contributors/18605/)
* [Jeffrey R. Bates](http://www.lexology.com/18605/author/Jeffrey_R_Bates/), [M. Leeann Habte](http://www.lexology.com/18605/author/M_Leeann_Habte/), [Leigh C. Riley](http://www.lexology.com/18605/author/Leigh_C_Riley/), [R. Michael Scarano Jr](http://www.lexology.com/18605/author/R_Michael_Scarano_Jr/), [Lawrence W. (Larry) Vernaglia](http://www.lexology.com/18605/author/Lawrence_W__Larry_Vernaglia/) and [Michael H. Woolever](http://www.lexology.com/18605/author/Michael_H_Woolever/) January 24 2013
* [](http://www.foley.com/)

[[](http://www.lexology.com/18605/author/Jeffrey_R_Bates/)Author page »](http://www.lexology.com/18605/author/Jeffrey_R_Bates/) [[](http://www.lexology.com/18605/author/M_Leeann_Habte/)Author page »](http://www.lexology.com/18605/author/M_Leeann_Habte/) [[](http://www.lexology.com/18605/author/Leigh_C_Riley/)Author page »](http://www.lexology.com/18605/author/Leigh_C_Riley/) [[](http://www.lexology.com/18605/author/R_Michael_Scarano_Jr/)Author page »](http://www.lexology.com/18605/author/R_Michael_Scarano_Jr/) [[](http://www.lexology.com/18605/author/Lawrence_W__Larry_Vernaglia/)Author page »](http://www.lexology.com/18605/author/Lawrence_W__Larry_Vernaglia/) [[](http://www.lexology.com/18605/author/Michael_H_Woolever/)Author page »](http://www.lexology.com/18605/author/Michael_H_Woolever/)

On January 17, 2013, the Office for Civil Rights of the U.S. Department of Health and Human Services (HHS) issued the long-awaited omnibus final rule (the Rule) implementing changes in current regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), pursuant to the Health Information Technology for Economic and Clinical Health Act (HITECH Act). Most of the Rule finalizes numerous proposed regulations set forth in a proposed rule dated July 14, 2010 (the Proposed Rule), which focused on the HITECH Act but also addressed other HIPAA provisions. The Rule also finalizes a proposed rule issued in 2009 that implements the HIPAA-related genetic privacy provisions of the Genetic Information Nondiscrimination Act (GINA).

The changes in the 563-page Rule are far-reaching and significantly strengthen privacy protections for patient health information, while enhancing HHS’ ability to enforce such protections. The Rule is effective on March 26, 2013, but Covered Entities1 and Business Associates subject to the Rule (collectively, Regulated Entities) are not required to comply with most of the Rule’s provisions until 180 days later, which is September 23, 2013. Below we provide an Executive Summary of the Rule, followed by a more detailed discussion. We conclude with our recommendations for preparing to comply.

**Executive Summary**

The most significant provisions in the Rule are summarized as follows:

**Business Associates.** As expected, the Rule extends the reach of HIPAA to a broad range of entities that were not previously covered. First, the Rule significantly expands the definition of “Business Associate” to include downstream Subcontractors of Business Associates and certain other entities. Second, it requires Business Associates to come into compliance with certain requirements of the HIPAA Privacy and Security Rules by September 23, 2013. Third, it imposes direct liability on Business Associates for violations of such provisions, with maximum civil fines of up to $1.5 million per year. (For a copy of Foley’s *Road Map for Business As*sociates, which provides guidance on what Business Associates should do to prepare for the new rules, contact one of the Foley attorneys listed at the end of this *Legal News Alert* or the Foley attorney with whom you regularly work.)

**Breach Notification.** The Rule significantly modifies the Breach Notification rules to limit the discretion of Regulated Entities to decide whether or not a Breach must be reported. A revised definition of “Breach” clarifies that an impermissible use or disclosure of Protected Health Information (PHI) is presumed to be a Breach, unless the Regulated Entity can prove otherwise. Further, the “harm standard” (which was the core of the existing risk analysis) is replaced by a four-factor analysis that HHS characterizes as a more objective standard.

**Marketing.** The Rule dramatically changes the definition of marketing and restricts Covered Entities from sending communications about health-related products or services that are subsidized by a third party (with the exception of prescription refill reminders) to patients without authorization.

**Other Privacy Rule Changes.** The Rule modifies authorization and other requirements to facilitate research and disclosure of child immunization information to schools, and to enable access to decedent information by family members or others.

**Individual Rights.** The Rule requires Covered Entities to make changes in their Notices of Privacy Practices (NPPs) to ensure that individuals are aware of the additional privacy protections and individual rights that were included in the HITECH Act. It also requires that a Covered Entity comply with an individual’s request to withhold disclosure of his or her PHI to a health plan for care that the individual paid for out of pocket.

**GINA.** The Rule modifies the HIPAA Privacy Rule to prohibit most health plans from using or disclosing genetic information for underwriting purposes. For the most part, the Rule adopts the substantive requirements and definitions that were included in the proposed GINA rule published in October 2009.

**Enforcement.** The Rule establishes more stringent fines and other enhancements to the government’s ability to enforce the HIPAA Privacy, Security, and Breach Notification rules.

**Discussion of the Rule**

**Business Associates**

**Business Associate Definition.** To incorporate changes made by the HITECH Act, the Rule expands the definition of Business Associate to include (1) a Health Information Organization (HIO), E-Prescribing Gateway, or other person that provides data transmission services with respect to PHI to a Covered Entity and that requires access on a routine basis to such PHI; (2) a person who offers personal health records to individuals on behalf of a Covered Entity; and (3) a Subcontractor that creates, receives, maintains, or transmits PHI on behalf of the Business Associate.

One of the most significant revisions made by the Rule is that Subcontractors of Business Associates, including those downstream Subcontractors that provide services on their behalf that involve PHI, must comply with certain HIPAA Security, Privacy, and Breach Notification requirements. Although the term “Subcontractor” is used, the definition applies to any person who performs functions or services on behalf of a Business Associate (other than in the capacity of a workforce member) that involve the use or disclosure of PHI, even if no contract between the parties exists.

HHS declines to define an HIO in regulation, but notes that the determination of whether a data transmission service would be considered a Business Associate versus a mere “conduit” that accesses PHI on a random or infrequent basis will be fact-specific. However, HHS emphasizes that it interprets the conduit exception very narrowly to apply only to transmission services (whether digital or hard copy), including any temporary storage of information incident to such transmission.

The Rule clarifies that the definition of Business Associate does not include health care providers that receive PHI for treatment purposes, plan sponsors that receive PHI from a group health plan under certain conditions, or government agencies that receive or collect PHI to determine eligibility for or enrollment in a government health plan that provides public benefits. In addition, to conform to the statutory provisions of the Patient Safety and Quality Improvement Act of 2005 (PSQIA), the definition adds patient safety activities to the list of functions and activities that give rise to a Business Associate relationship.

**Application of the Privacy and Security Rule to Business Associates.** Under the current Privacy Rule, Business Associates are contractually obligated to comply with the terms of their Business Associate Agreements with Covered Entities, which include certain privacy and security requirements, but are not directly liable to HHS for violations. The HITECH Act makes Business Associates directly subject to certain provisions of the Privacy and Security rules and creates direct liability on the part of Business Associates for violations.

The Rule makes Business Associates subject to the administrative, physical, and technical safeguards requirements of the Security Rule (45 C.F.R. §§ 164.306, 164.308, 164.310, and 164.312) as well as the policies and procedures and documentation requirements in § 164.316. These Security Rule requirements are applied to Business Associates in the same manner as these requirements apply to Covered Entities, which means that Business Associates may be held civilly and criminally liable for penalties for violations of these provisions.

Similarly, the Rule applies certain privacy requirements to Business Associates and creates direct liability for Business Associates for violations of these provisions of the Privacy Rule. A Business Associate is not liable for compliance with the entire Privacy Rule, but is directly liable for:

* Uses and disclosures of PHI that are not in accordance with its Business Associate Agreement or the Privacy Rule
* Failure to disclose PHI to HHS for compliance purposes
* Failure to disclose PHI to an individual, or the individual’s designee in order for the Covered Entity to comply with its obligations to provide electronic access to PHI
* Failure to comply with the minimum necessary standard
* Failure to enter into Business Associate Agreement with Subcontractors

HHS clarifies that liability attaches to an entity that meets the definition of a Business Associate, irrespective of whether the entity has entered into a contract with a Covered Entity or another Business Associate. Further, liability does not depend on the type of PHI that the Business Associate creates, receives, transmits, or maintains on behalf of a Covered Entity or another Business Associate, or on the type of entity performing the function or services, unless the entity falls within one of the exceptions to the definition of a Business Associate. If the information is tied to a Covered Entity (even if it is limited to demographic information), it is PHI by definition because it is indicative that the individual received services from the Covered Entity. Therefore, such information must be protected in accordance with the applicable provisions of the HIPAA Privacy, Security, and Breach Notification Rules and the terms of the applicable Business Associate Agreement.

**Business Associate Agreements.** The Rule expands the required elements of Business Associate Agreements to include provisions requiring that Business Associates: (1) comply, where applicable, with the Security Rule with regard to electronic PHI; (2) report Breaches of Unsecured PHI to Covered Entities; and (3) 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 with respect to such information.

The Rule also indicates that if a Covered Entity and Business Associate have failed to enter into a Business Associate Agreement or other arrangement, the Business Associate may only use or disclose PHI as necessary to perform its obligations to the Covered Entity or as required by law. Covered Entities have no new obligation to enter into Business Associate Agreements with Subcontractors; that obligation falls solely on Business Associates; however, Covered Entities must require their Business Associates to comply with this obligation.

The Rule removes the requirement that Covered Entities report to HHS when a Covered Entity is aware of noncompliance by a Business Associate and is unable to cure the Breach, and termination of a Business Associate Agreement is not feasible. Finally, the Preamble to the Rule (Preamble) emphasizes that in addition to having direct liability for impermissible uses and disclosures of PHI, Business Associates are still contractually liable to Covered Entities pursuant to their Business Associate Agreements with respect to the performance of any activities that are not directly imposed on Business Associates by the HIPAA Rules.

**Transition Provisions.** The Rule provides some relief of the burden of compliance with the revised Business Associate provisions by adding a transition provision to “grandfather” certain existing Business Associate Agreements for a specified period of time. The Rule adds transition provisions to allow Regulated Entities (including Subcontractors) to continue to operate under certain existing contracts for up to one year beyond the compliance date of the Rule. HHS will deem such contracts to be compliant with the modifications in the Rule until either the Covered Entity or Business Associate has renewed or modified the contract following the compliance date of the modifications, or until the date that is one year after the compliance date, whichever is sooner.

**Security Breach Notification**

The Interim Final Rule dated Aug. 24, 2009 (Breach Notification Rule) added a new subpart D to part 164 of title 45 of the Code of Federal Regulations to implement the Breach Notification provisions established in the HITECH Act. In the Breach Notification Rule, a “Breach” was defined as “the acquisition, access, use, or disclosure of protected health information in a manner not permitted under Subpart E of this part [the Privacy Rule] which compromises the security or privacy of the PHI,” with certain exceptions. For purposes of this definition, the Breach Notification Rule provided that “compromises the security or privacy of the protected health information” means that a disclosure poses a significant risk of financial, reputational, or other harm to the affected individual. Under this approach, a Covered Entity or Business Associate is required to conduct a risk analysis to evaluate whether an impermissible use or disclosure satisfied the “harm standard.”

In the Rule, HHS significantly revises the risk assessment approach described in the Breach Notification Interim Rule. First, HHS adds language to the definition of Breach to clarify that an impermissible use or disclosure of PHI is presumed to be a Breach unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised. HHS emphasized that the burden is on the Covered Entity or Business Associate to prove that there is a low probability that the information has been compromised. Second, HHS abandons the “harm standard” in favor of a four-factor risk assessment approach that focuses more objectively on the risk that the PHI has been compromised. HHS retains the exceptions to the definition of a Breach established in the Breach Notification Rule, including the unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of the Covered Entity, the inadvertent disclosure of information by an authorized person to another person authorized to access PHI at the same Covered Entity, Business Associate, or Organized Health Care Arrangement, and unauthorized disclosures where the person receiving the information would not reasonably have been able to retain it.

To determine whether there is a low probability that the information has been compromised, the Covered Entity or Business Associate must conduct a risk assessment that considers at minimum, the following four 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
* The extent to which the risk to the PHI has been mitigated

Regulated Entities must then evaluate the overall probability that the PHI has been compromised by considering all the factors in combination. In the Preamble, HHS emphasizes that it expects such risk assessments to be thorough and completed in good faith, and the conclusions reached to be reasonable. If an evaluation of the factors discussed above fails to demonstrate that there is a low probability that the PHI has been compromised, Breach Notification is required.

The Rule also removes the exception to the Breach Notification requirement for a limited data set that excludes dates of birth and zip code. However, the timing requirements for Breach Notification, the content of the Breach Notification, and the nature of the Breach Notification requirements remain essentially unchanged. Regarding the timing of Breach Notification, the Preamble clarifies that the Business Associate’s discovery of a Breach will be imputed to the Covered Entity if the Business Associate is acting as an agent of the Covered Entity.

**Privacy Rule**

**Marketing.** The Privacy Rule currently requires a Covered Entity to obtain an individual authorization in order to use or disclose PHI for marketing purposes. “Marketing” is defined as “a communication about a product or service that encourages recipients of the communication to purchase or use the product or service,” subject to exceptions for certain health-related communications. These exceptions apply irrespective of whether payments from a third party are received in exchange for making the communications. The Privacy Rule does not require a Covered Entity to obtain individual authorization for face-to-face communications or to provide only promotional gifts of nominal value to the individual. However, a Covered Entity must obtain prior written authorization from an individual to send communications to the individual about non-health related products or services or to give or sell the individual’s PHI to a third party for marketing.

The HITECH Act enacts limitations on the health-related communications that are excepted from the definition of “marketing” under the Privacy Rule, to the extent a Covered Entity receives or has received direct or indirect payment in exchange for making the communication. According to HHS, Congress intended that these provisions curtail a Covered Entity’s ability to send communications to the individual that are motivated more by commercial purposes rather than for the individual’s health care, despite the communication being about a health-related product or service.

The Proposed Rule proposed exceptions to the definition of marketing for the following:

* Treatment communications, conditioned on notice, and an opportunity to opt out
* To provide refill reminders or to 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 in exchange for making the communication is reasonably related to the Covered Entity’s cost in making the communication
* To describe a health-related product or service that is provided by, or included in the plan of benefits, of the Covered Entity making the communication, or for case management, care coordination, or contacting individuals with information about treatment alternatives and related functions, as long as the Covered Entity does not receive financial remuneration in exchange for making the communication

The Rule significantly departs from the Proposed Rule’s approach to marketing by eliminating the exception for treatment communications. It requires authorization for all treatment and health care operations communications if the Covered Entity receives financial remuneration in exchange for making the communication from a third party whose product or service is being marketed.

“Financial remuneration” for purposes of the Rule is defined as “direct or indirect payment from or on behalf of a third party whose product or service is being described.” Direct or indirect payment does not include any payment for treatment of an individual. HHS clarifies that direct payment means financial remuneration that flows from the third party whose product or service is being described directly to the Covered Entity, whereas indirect payment means financial remuneration that flows from an entity on behalf of the third party whose product or service is being described to a Covered Entity. Financial remuneration does not include in-kind services; a payment must be involved. The payment must be in exchange for making the communication and not for other purposes. HHS further clarifies that individual authorization also is required if a Business Associate is making such communication on behalf of a Covered Entity.

In order to make a marketing communication to an individual, a valid authorization is required, and the authorization must disclose the fact that remuneration is being received from a third party for making the communication. The scope of the authorization need not be limited to subsidized communications related to a single product or service or the products or services of one third party, but rather may apply more broadly to subsidized communications generally so long as the authorization adequately describes the intended purposes of the requested uses and disclosures (i.e., the scope of the authorization) and otherwise contains the elements and statements of a valid authorization under 45 C.F.R. § 164.508.

The exceptions for face-to-face communications and promotional gifts of nominal value set forth in the Privacy Rule remain. According to HHS, this means that a provider could recommend an alternative medication verbally or could hand out a pamphlet in a face-to-face communication, even if the provider received payment from a third party in exchange for making that communication. However, communications over the phone or by email do not constitute face-to-face communication, and thus, an authorization would be necessary.

The Rule also maintains the proposed exception for refill reminders or to otherwise communicate about a drug or biologic that is currently being prescribed for an individual, provided that any financial remuneration received by the Covered Entity in exchange for making the communication is reasonably related to the Covered Entity’s costs of making the communication. In the Preamble, HHS clarifies the scope of the exception and what constitutes permissible costs. HHS states that the exception extends to communications about the generic equivalent of a drug being prescribed to an individual as well as adherence communications encouraging individuals to take their prescribed medication as directed. Additionally, the exception applies to prescriptions for self-administered drugs or biologics and communications regarding all aspects of a drug delivery system. HHS also explains that the permissible costs for which a Covered Entity may receive remuneration under this exception are those that cover only the costs of labor, supplies, and postage to make the communication. Where the financial remuneration a Covered Entity receives in exchange for making the communication generates a profit or includes payment for other costs, such financial remuneration would run afoul of the HITECH Act’s “reasonable in amount” language.

**Sale of PHI.** To implement the HITECH Act, and consistent with the Proposed Rule, the Rule prohibits a Covered Entity or Business Associate from receiving direct or indirect remuneration in exchange from or on behalf of the recipient of the PHI in exchange for the PHI, unless the Covered Entity or Business Associate has obtained a valid authorization from the individual. The authorization obtained by a Covered Entity for any such disclosure of PHI must state that the disclosure will result in remuneration to the Covered Entity. HHS provides discretion to Covered Entities to craft language that reflects the nature of the remuneration.

The Rule contains several exceptions to this authorization requirement. The authorization requirement does not apply to disclosures of PHI:

* For public health purposes
* For research purposes where the only remuneration received by the Covered Entity is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes
* For treatment and payment purposes
* For the sale, transfer, merger, or consolidation of all or part of the Covered Entity and related due diligence
* To or by a Business Associate for activities that the Business Associate undertakes on behalf of a Covered Entity and the only remuneration provided is by the Covered Entity to the Business Associate for the performance of such activities
* To an individual, when requested under the access and accounting of disclosures provisions of the Privacy Rule
* For disclosures required by law
* For any other purpose permitted by and in accordance with the applicable requirements of the Privacy Rule, where the only remuneration received by the Covered Entity is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law

Ongoing research studies will be grandfathered, and a Covered Entity may continue to use a Limited Data Set in accordance with an existing data use agreement until the data use agreement is renewed or modified or until one year from the compliance date of the Rule, whichever is earlier, even if such disclosure would otherwise constitute a sale of PHI upon the effective date of the Rule.

**Fundraising.** The Rule generally adopts the provisions of the Proposed Rule with respect to fundraising, and also allows certain additional types of PHI to be used for fundraising purposes. It establishes the following requirements:

* A Covered Entity must provide, with each fundraising communication, a clear and conspicuous opportunity to opt out of receiving future fundraising communications; HHS notes that Covered Entities are free to determine the method that an individual may use to opt out, as long as it does not cause undue burden to the individual
* A Covered Entity cannot condition treatment or payment on an individual’s choice to receive or not to receive fundraising communications
* When individuals have opted out of receiving fundraising communications, the Covered Entity may not send such information to them, as opposed to the previous Privacy Rule requirement to make “reasonable efforts” not to send such information

A Covered Entity may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications. In the Rule, HHS also expands the information that can be used and disclosed for fundraising to include date of birth, department of service, treating physician information, outcome information, and health insurance status.

**Research.** Under the current Privacy Rule, a Covered Entity may condition the provision of certain research-related treatment on the research subject’s agreement to execute an authorization for disclosure of PHI. In such circumstances, it is permissible for a Covered Entity to utilize a “compound authorization” (i.e., a document that combines the subject’s consent to participate in the research trial with the subject’s authorization to disclose the subject’s PHI). However, when a research trial includes both research-related treatment and a corollary activity, such as the banking of tissue (and associated PHI), Covered Entities must obtain separate authorizations from a research subject, (i.e., one authorization for research-related treatment, which may be combined with the research consent) and a separate authorization for tissue banking.

The Rule eliminates the requirement for a separate document in these and certain other circumstances, as long as certain requirements applicable to the document used in obtaining the compound authorization are met. In particular, that document must clearly differentiate between the authorization associated with research-related treatment and the authorization associated with the corollary activity. Further, the document must clearly permit the subject to opt in to the authorization associated with the corollary activity. However, the Rule provides flexibility to Covered Entities and institutional review boards to determine the best approach for differentiating the two types of research activities and giving research participants the option to opt in to the corollary activity.

In the Preamble, HHS also changes its prior interpretation that research authorizations for future research must be study-specific. Instead, an authorization for future research will be deemed sufficient if it includes a description of each purpose of the requested future use or disclosure that adequately describes such purpose such that it would be reasonable for an individual to expect that his or her PHI could be used or disclosed for such future research.

**PHI of Decedents.** The Privacy Rule currently requires Covered Entities to protect the privacy of a decedent’s PHI indefinitely, generally in the same manner as is required for the PHI of living individuals. The Rule makes two significant changes affecting the PHI of deceased individuals.

First, the Rule revises the definition of PHI to exclude individually identifiable health information of a person who has been deceased for more than 50 years. This change responds to concerns expressed to HHS that it can be difficult to locate a personal representative to authorize the use or disclosure of decedent’s PHI after an extended period of time. HHS states that 50 years — roughly two generations — is a sufficient amount of time to protect the privacy interests of most, if not all, living relatives or other affected individuals.

Second, the Rule addresses concerns that family members and others who have had access to PHI of a deceased individual prior to death often have difficulty obtaining such access following the individual’s death. This is because these individuals often do not fall within the definition of “personal representative” in the Privacy Rule. The Rule modifies the Privacy Rule to permit Covered Entities to disclose the decedent’s information to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the Covered Entity.

**School Immunizations.** Under current law, a written authorization is required for Covered Entities to disclose immunization records to schools. The Rule adds a new provision that permits the Covered Entity to disclose proof of immunization to a school where state or other law requires the school to have such information prior to admitting the student. While written authorization will no longer be required to permit such disclosures, Covered Entities will still be required to obtain oral agreement from a parent or guardian or, if the individual is an adult or an emancipated minor, from the individual.

**Organizational Requirements for Hybrid Entities.** The Rule clarifies certain issues relative to Hybrid Entities, which are defined in the Privacy Rule as entities that perform both HIPAA-covered and non-covered functions as part of their business operations. With respect to a Hybrid Entity, the Rule clarifies that the Covered Entity itself (i.e., the legal entity), and not merely the designated health care component, remains responsible for complying with the security rules regarding Business Associate arrangements and other organizational requirements. With respect to a Hybrid Entity, however, not including Business Associate functions within the health care component of a Hybrid Entity could avoid direct liability and compliance obligations for the Business Associate component. Therefore, the Rule requires that the health care component of a Hybrid Entity include all Business Associate functions within the entity.

**Individual Rights**

**Notice of Privacy Practices.** The Privacy Rule currently requires most Covered Entities to have and distribute an NPP to individuals. The NPP must describe the uses and disclosures of PHI that a Covered Entity is permitted to make, the Covered Entity’s legal duties and privacy practices with respect to PHI, and the individual’s rights concerning PHI.

To ensure that individuals are aware of the HITECH Act changes that affect privacy protections and individual rights regarding PHI, the Rule requires Covered Entities to make a number of material changes to their NPPs. The NPP must contain information regarding the uses and disclosures that require authorization, and include specific statements indicating that:

* Uses and disclosures of PHI for marketing purposes, as well as disclosures that constitute a sale of PHI, require authorization by the individual
* Other uses and disclosures not described in the NPP will be made only with authorization from the individual
* PHI will be used and disclosed for fundraising communications (if a Covered Entity intends to contact an individual to raise funds for the Covered Entity), and individuals have a right to opt out of receiving such communications
* Individuals have a right to restrict certain disclosures of PHI to a health plan where the individual pays out of pocket in full for the health care item or service; only health care providers are required to include such a statement in the NPP — other Covered Entities may retain the existing language indicating that a Covered Entity is not required to agree to a requested restriction on the disclosure of PHI
* Affected individuals have a right to be notified following a Breach of unsecured PHI; HHS clarified that a simple statement in the NPP that an individual has a right to or will receive notifications of Breach of his or her unsecured PHI will suffice for purposes of this requirement

In addition, Covered Entities that record or maintain psychotherapy notes will be required to include in the NPP a specific statement that most uses and disclosures of psychotherapy notes require authorization.

Health care providers will continue to be subject to the current requirements regarding distribution of revised NPPs.

**Right to Request a Restriction of Uses and Disclosures.** The current Privacy Rule requires Covered Entities to permit individuals to request that a Covered Entity restrict uses or disclosures of their PHI, but does not require the Covered Entity to agree to such requests. If the Covered Entity agrees to a restriction, the Covered Entity must document the restriction and abide by the restriction (except in emergencies). A Covered Entity may terminate its agreement to a restriction in certain circumstances.

The HITECH Act sets forth certain circumstances in which a Covered Entity must comply with an individual’s request for restriction of disclosure of his or her PHI. Under the Rule, a Covered Entity, upon request from an individual, must agree to a restriction on the disclosure of PHI to a health plan if: (1) the disclosure of PHI would be for the purposes of carrying out payment or health care operations, and is not otherwise required by law; and (2) the PHI pertains solely to a health care item or service for which the individual, or a person acting on behalf of the individual (other than the health plan), has paid the Covered Entity in full. HHS clarified that providers continue to be allowed to make disclosures that are otherwise required by law, notwithstanding than an individual has requested a restriction on such disclosures.

In the Rule, HHS states that it is the individual’s, and not the provider’s, obligation to notify downstream health care providers of restrictions on the disclosure of PHI. HHS states that it would be unworkable at this point, given the lack of automated technologies to support such a requirement, to require health care providers to notify downstream providers of the fact that an individual has requested a restriction on the disclosure of PHI to a health plan.

**Access to PHI by Individuals.** The Privacy Rule currently establishes the right of individuals to review or obtain copies of their PHI, to the extent such information is maintained in the designated record set of a Covered Entity. An individual’s right of timely access exists regardless of whether the PHI is in electronic or paper format. The HITECH Act strengthens the Privacy Rule’s right of access to PHI that is maintained in an electronic health record (EHR).

The Rule amends the Privacy Rule to require that if an individual requests an electronic copy of PHI that is maintained electronically in one or more designated record sets, the Covered Entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible or, if not, in a readable electronic form and format as agreed to by the Covered Entity and the individual. This requirement will apply uniformly to all electronic PHI maintained in a designated record set held by a Covered Entity, regardless of whether the record is maintained in an EHR or another electronic format. HHS states that a Covered Entity will not be required to purchase new software or systems in order to accommodate an electronic copy request for a specific format that is not readily producible by the Covered Entity at the time of the request, provided that the Covered Entity is able to provide some form of electronic copy.

The HITECH Act provides that, if requested by an individual, the Covered Entity must transmit an electronic copy of PHI in an EHR directly to an entity or person designated by the individual, provided that such choice is clear, conspicuous, and specific. The Rule applies this requirement to information in both paper and electronic form, and specifies that the individual’s request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the PHI.

The Privacy Rule currently permits a Covered Entity to impose a reasonable, cost-based fee for a copy of PHI, which may include the costs of the supplies for, and labor for, copying the PHI; the postage associated with mailing the PHI, if applicable; and the preparation of an explanation or summary of the PHI, if agreed to by the individual. In the Rule, HHS acknowledges commenters’ assertions that the cost related to searching for and retrieving electronic PHI in response to requests would be not be negligible, as opposed to what HHS had anticipated in the Proposed Rule, particularly in regards to designated record set access that will require more technically trained staff to perform this function. HHS clarifies that labor costs included in a reasonable cost-based fee could include skilled 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. The Rule also allows a Covered Entity to charge for the cost of supplies for creating the paper copy or electronic media, if the individual requests that the electronic copy be provided on portable media; and the cost of postage, if the individual requests that the portable media be sent by mail or courier. A standard retrieval fee that does not reflect the actual labor costs related to an individual’s request is not allowable.

**The Enforcement Rule**

The Rule makes a number of modifications to the HIPAA Enforcement Rule, most of which are required by the HITECH Act. The Rule requires HHS to investigate any complaint or other source if information comes to its attention (e.g., a media report) and a preliminary review of the facts indicates a “possible” violation due to willful neglect. HHS will continue to have discretion to conduct investigations where the circumstances do not indicate willful neglect. Further, the Rule requires HHS to impose a penalty on a Regulated Entity if, following its investigation, HHS determines that a violation occurred due to willful neglect that was not cured within 30 days of when the entity discovered, or should have discovered, the violation.

The Rule also includes certain changes to the HIPAA Enforcement Rule that were initially promulgated as part of an interim final rule issued in October 2009. These include provisions establishing four categories of violations reflecting four levels of culpability and four corresponding tiers of penalty amounts, with minimum fines ranging from $100 to $50,000 per violation and maximum fines of $1.5 million for all violations of the same standard during any year. The lowest category of violation with the lowest penalty covers situations where the entity did not know, and by the exercise of reasonable diligence would not have known, of the violation. The second lowest category applies to violations due to reasonable cause and not willful neglect. The third category applies to circumstances where the violation was due to willful neglect and was corrected within 30 days of when the entity knew, or should have known, of the violation; and the fourth category corresponds to violations due to willful neglect that are not corrected within the same 30-day period. The Rule also clarifies the state of mind (mens rea) associated with each penalty tier and sets forth the factors HHS will take into account in establishing the amount of the penalty in any given case.

The Rule eliminates an affirmative defense that currently protects a Covered Entity from liability for the acts of its Business Associate in cases where the Business Associate is an agent of the Covered Entity, the relevant Business Associate contract requirements have been met, the Covered Entity did not know of a pattern or practice of the Business Associate in violation of the contract, and the Covered Entity did not fail to act. Instead, the Rule specifically provides for civil money penalty liabilities against a Covered Entity for the acts of its Business Associate, regardless of whether the Covered Entity knew of the violation or had a compliant agreement in place, if the Business Associate is an agent of the Covered Entity. The Preamble states that a Business Associate will not always be an agent of its Covered Entity, and that the government would apply the federal common law definition of agent in determining whether that is the case. Under that standard, the most important factor is the Covered Entity’s right to control the Business Associate.

**GINA-Related Changes in the Rule**

In addition to incorporating changes required under the HITECH Act, the Rule also modifies the HIPAA Privacy Rule to incorporate the requirements of section 105 of Title I of the Genetic Information Nondiscrimination Act of 2008. As is the case with the HITECH Act changes, the GINA-related changes to the HIPAA Privacy Rule are effective March 26, 2013 with full compliance being required 180 days later.

Generally speaking, GINA prohibits discrimination based on an individual’s genetic information in both the health coverage and employment contexts. With respect to health coverage, GINA prohibits discrimination in premiums or contributions for group coverage based on genetic information, proscribes the use of genetic information as a basis for determining eligibility or setting premiums in the individual and Medicare supplemental (Medigap) insurance markets, and limits the ability of group health plans, health insurance issuers, and Medigap issuers to collect genetic information or to request or require that individuals undergo genetic testing.

GINA Section 105 contains two additional privacy protections for genetic information. First, Section 105 requires HHS to revise the HIPAA Privacy Rule to clarify that genetic information is health information. Second, Section 105 prohibits group health plans, health insurance issuers (including HMOs), and Medigap issuers from using or disclosing genetic information for underwriting purposes.2

Although HHS had issued informal guidance in 2002 stating that for privacy purposes health information includes genetic information, the informal guidance did not define the term “genetic information.” However, that term, as well as other key terms such as “family member,” “genetic services,” and “genetic test” were defined in GINA and in the regulations jointly promulgated by the HHS, the Internal Revenue Service, and the U.S. Department of Labor under Sections 101-103 of GINA implementing GINA’s non-discrimination rules (Joint Non-Discrimination Rules).

When HHS published a proposed GINA amendment to the HIPAA Privacy Rule in October 2009, the proposal incorporated these key GINA-related definitions. These definitions are included in the Rule without major modification. Thus, Covered Entities now have clear final guidance on the nature and scope of genetic related information that is protected under the HIPAA Privacy Rule.3

The term “genetic information” is defined to mean, with respect to any individual, information about: (1) such individual’s genetic tests; (2) the genetic tests of family members of such individual; and (3) the manifestation of a disease or disorder in family members of such individual (i.e., family medical history). It also includes not only, for example, the results of a genetic test, but also any request for, or receipt of, genetic services, or participation in clinical research that includes genetic services, by such individual or any family member. The definition of “genetic services” in the Rule includes not only genetic tests, but also genetic counseling or genetic education. Thus, the fact that an individual or a family member of the individual requested or received a genetic test, counseling, or education is itself information protected under GINA and the Privacy Rule.

The term “genetic test” is defined to mean “an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, that detects genotypes, mutations, or chromosomal changes,” but excludes an analysis of proteins or metabolites that does not detect genotypes, mutations, or chromosomal changes or an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition that could reasonably be detected by a health care professional with appropriate training and expertise in the field of medicine involved.

The Rule also adopts the definitions of the term “family member” (including a fourth degree relative) from the proposed amendment without change. Like the other definitions discussed above, this definition conforms to the definition of the term “family member” in the Joint Non-Discrimination Regulations and, consistent with the legislative history of GINA, is a very inclusive definition.

When updating their policies and procedures to conform to the HITECH Act amendments to the HIPAA Privacy Rule, health plans, as well as other Covered Entities, will want to review their policies and procedures to ensure that they are fully complying with the HIPAA Privacy Rule when it comes to the use and protection of genetic information. In doing so, health plans will need to be aware of the fact that some types of uses of protected information that are permitted under the HIPAA Privacy Rule with respect to non-genetic health information do not apply to genetic information due to application of the prohibition on the use of genetic information for “underwriting purposes,” which is defined in the Rule to include:

* Determining eligibility or coverage under a plan, coverage or policy or benefits under a plan coverage or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program)
* Premium contributions (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program)
* Application of any pre-existing condition exclusion under the plan, coverage, or policy
* Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits

For example, while Section 164.504(f)(1)(ii) permits a group health plan, or health insurance issuer or HMO with respect to the group health plan, to disclose summary health information to the plan sponsor if the plan sponsor requests the information for the purpose of obtaining premium bids from health plans for providing health insurance coverage under the group health plan, or for modifying, amending, or terminating the group health plan, the Rule has modified § 164.504(f)(1)(ii) to clarify that § 164.504(f)(1)(ii) would not allow a disclosure of PHI that is otherwise prohibited by the underwriting prohibition (i.e., genetic information).

Finally, health plans should note that the Rule also requires that the Notice of Privacy Practices issued by a health plan that engages in underwriting, consistent with the rules in the Rule regarding material changes to the NPP, include a specific reference to the fact that the health plan is prohibited from using or disclosing PHI that is genetic information about an individual for such purposes.

**Pending Rules**

The Rule does not address the accounting for disclosures requirements, which is the subject of a separate proposed rule published on May 31, 2011, or the penalty distribution methodology requirement. HHS has stated that both of these issues will be the subject of future rulemaking.

**Recommendations**

Although Regulated Entities have until September 23, 2013 to come into full compliance with the Rule, we recommend that Covered Entities and Business Associates begin preparing soon, as the Rule imposes a number of new or enhanced compliance obligations. Covered Entities will need to revise their Business Associate Agreements (although they have up to a year beyond the compliance date of September 23, 2013 to revise their **existing** agreements); revise their NPPs; and revise certain Privacy, Security, and Breach Notification policies to reflect these new regulatory requirements. We further recommend that Covered Entities carefully evaluate any subsidized communication arrangements to make sure that they comply with the new marketing restrictions. Covered Entities also may wish to develop and implement new patient authorization forms to address marketing, sale of PHI, and fundraising communications.

Business Associates face the daunting task of preparing to comply with the HIPAA Privacy and Security rules. As a first step to compliance with the Security Rule, Business Associates will need to conduct a security risk assessment and implement a written HIPAA Security Plan. They also will need to adopt certain HIPAA privacy policies. In addition, Business Associates will be required to develop, negotiate, and implement Business Associate Agreements with Subcontractors who meet the expanded definition of Business Associate.