The Wait is Over:  
HHS Issues Final Rules that Significantly Expand HIPAA Privacy and Security Regulations

On January 25, 2013, the Department of Health and Human Services (HHS) issued significant modifications to the HIPAA privacy, security, and enforcement regulations. 78 Fed. Reg. 5566. The new rules, which are in final form, are applicable as of September 23, 2013, although there are some transition rules that allow for longer compliance times (as discussed below).

The new final rules will impact who is a business associate and business associate agreements, HIPAA privacy notices, the security breach notification rules, marketing communications, and an individual’s right to access or restrict protected health information (PHI). The new final rules also expand enforcement, including making covered entities liable for acts of a business associate where an “agency” relationship exists and making business associates directly liable for a number of privacy and security requirements, rather than just having contractual liability under a Business Associate Agreement (BAA). In addition, the new final rules treat certain violations under the Genetic Information Nondiscrimination Act (GINA) as HIPAA privacy violations as well, which means greatly increased potential penalties under GINA.

We have summarized below the major areas that will impact employer-sponsored health plans and health insurance issuers - broken out into ten major sections - along with our practical observations.

I. Business Associates
II. Right to Access PHI
III. Right to Restrict Disclosures of PHI
IV. Security Breach Notifications
V. Using PHI for Marketing Purposes / Sale of PHI
VI. Disclosure of Deceased Individual’s Information To Family Members
VII. Genetic Information / GINA Interaction
VIII. Updates to HIPAA Privacy Notice
IX. Increased Enforcement
X. Other Provisions- Other Individual Rights, Student Immunization Information, Hybrid Entity Rules, Fundraising Communications
Background

HHS first issued HIPAA privacy rules in 2000 and HIPAA security rules in 2003. Both rules apply to covered entities - health plans, health care providers, and clearinghouses - and require covered entities to safeguard protected health information (PHI), which is defined as individually identifiable health information. Health plans must obtain an individual’s written authorization to use or disclose PHI, other than for purposes of treatment, payment, or health care operations or pursuant to an express exception, such as disclosures to respond to a subpoena; for law enforcement, research, or public health purposes; or, in limited cases, to family members or the health plan sponsor. Individuals have a host of rights to their own health information, including a right to access or amend health records, a right to an “accounting” of certain disclosures by the covered entity, and a right to request restrictions of disclosures. Health plans must provide individuals with a Notice of Privacy Practices that describes these restrictions and rights. Health plans also must have a BAA in place with any third party that acts on behalf of the plan in a function involving PHI. The BAA requires the third party service provider also to comply with many of the HIPAA requirements. In addition, health plans must implement privacy policies and procedures, train the plan’s workforce with regard to those policies and procedures, and appoint a privacy official.

The HIPAA security rules further require that covered entities provide administrative, physical, and technical safeguards for electronic PHI (ePHI). Plans are required to perform a risk assessment regarding a number of specific standards for ePHI, amend their BAAs and plan documents with respect to security requirements, and appoint a security official.

Following the passage of the HITECH Act in 2010, HHS issued security breach notification rules, which require health plans to notify an individual whose PHI has been breached and, in some cases, notify the media. The health plan also must notify HHS, which has used this information to initiate investigations and penalties.

For the most part, all of these rules have now been updated, as described below.

I. BUSINESS ASSOCIATES

Pre-HITECH:

The HIPAA privacy rules require that a covered entity have a business associate agreement (BAA) in place with any entity that acts on behalf of a covered entity in a function involving PHI. The privacy rules listed required information that must be included in a BAA, and the security rules added additional requirements.

What’s New:

- **BAAs May Need Updating** – In large part, the content of BAAs is the same under the final rules. However, the final rules include the following changes that must be incorporated into a BAA:
  - The business associate must agree to comply, where applicable, with the HIPAA security standards with respect to electronic PHI. (Before, this was not an express requirement, although most BAAs likely required compliance with all of HIPAA, so may not be a substantive difference.)
  - The business associate must agree to report any breaches of unsecured PHI as required under the security breach rules. (This requirement has been applicable since the interim final rule on security breach notifications, but not an express requirement of the BAA.)
- The business associate must require subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate to agree to the same restrictions and conditions as the business associate. (This language has been slightly re-worded from the prior rule.)

- The business associate must agree that, to the extent the business associate is to carry out a covered entity’s obligations under the privacy rule that it will comply with the requirements of the privacy rule that apply to the covered entity. (Again, this likely was included – or at least intended – in prior BAAs, but now is an express requirement.)

HHS has provided a sample BAA based on the new final rules at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

### Practical Observation: Many health plans updated their BAAs after the HIPAA security breach rules were issued and likely already include much of the “new” language that is required. So, some plans may have very little to update. However, we would suggest that all plans review their BAAs to verify that the content is still accurate under the final rules. For example, some BAAs go into detail about the right to access rule, which has changed somewhat (see below), so some BAA provisions may need to be updated, depending on the detail of the current language. In addition, plans should review contract and BAA language to see if the business associate could be considered the plan’s “agent,” which may cause additional liability and review or add indemnification language to account for this potential new liability (see below for more detail).

- **Transition Period for Updating BAAs** – While the general applicability date for the new rules is 9/23/13, the final rule provides a transition period for updating BAAs where there is already a BAA in place. These BAAs must be updated by the earlier of: (1) the next renewal after 9/23/13 or (2) 9/23/14. The Preamble clarifies that the HIPAA requirements apply in substance – the transition rule only applies to the documentation of these rules in the BAA.

This special transition rule only applies where there was a BAA in place as of 1/25/13 (the date the final rules were issued) and the underlying contract between the plan and business associate is not renewed between 3/26/13 (the “effective date” of the rules) and 9/23/13 (the “applicability date” of the rules). Plans and business associates that do renew their contracts between 3/26/13 and 9/23/13 must have a compliant BAA as of 9/23/13.

Any new BAAs entered into on or after 9/23/13 must meet the new requirements (but, as a practical matter, plans and business associates may want to use updated BAAs for agreements entered into prior to that date as well).

- **Subcontractors Also Need BAAs** - The new rules require that business associates not only have a BAA in place with the covered entity to whom they are providing services, but also with any subcontractors that use PHI of the covered entity. This is a new requirement that will significantly impact business associates and their subcontractors. The Preamble to the rules clarifies that subcontractors also will need BAAs with their subcontractors "no matter how far down the chain" as long as PHI is being used. In addition, the subcontractor BAA must be at least as stringent as the BAA above it. Business associates and subcontractors can use the same transition rules that apply to covered entities and base the applicability date of the subcontractor BAA on the covered entity’s contract renewal date with the business associate.
• **Data Transmission & Network Services** - The new rules state that a business associate includes a Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services to a covered entity that requires access to PHI on a “routine basis.” The Preamble clarifies that entities that manage the exchange of PHI through a network, including those providing record locator services or performing oversight and governance functions for an electronic health information exchange have more than "random access" and would be considered business associates.

• **Personal Health Record (PHR) Vendors** – The new rules also define a business associate to include a party offering PHRs on behalf of a covered entity. The Preamble clarifies that the rules do not apply to PHR vendors who are considered to act for the individual and who have an individual's authorization to access a covered entity's data, even if the PHR vendor has an agreement with the covered entity regarding the exchange of data, such as technical specifications.

• **Mere Conduit Exception** - Where a third party does not require access to PHI on a “routine basis,” it may be acting as a "mere conduit" for the transport of PHI and not be considered a business associate. The Preamble says that the "conduit" exception is narrow and intended to exclude only those entities providing mere courier service like the US Postal Service or UPS and their electronic equivalents, such as Internet service providers (ISPs) providing mere data transmission services. HHS says that whether the conduit exception applies is fact specific based on the nature of service provided. For example, a telecommunications company that has occasional random access to PHI to review whether data transmitted over its network arrives at its intended destination may be a conduit and, in that case, would not be considered a business associate.

• **Business Associate Liability** - Before HITECH, business associates were not directly liable for HIPAA violations and could not be penalized by HHS. They only were contractually liable to the covered entity via the BAA. Under HITECH and the new rules, business associates (as well as subcontractors) are directly liable and can be penalized by HHS for:
  
  - Impermissible uses and disclosures of PHI;
  
  - Failure to provide breach notification to the covered entity;
  
  - Failure to provide access to a copy of electronic PHI to the covered entity, the individual, or the individual’s designees (whichever is specified in the BAA);
  
  - Failure to disclose PHI where required by the Secretary to investigate or determine the business associate’s compliance with HIPAA;
  
  - Failure to provide an accounting of disclosures (under the proposed accounting rule, which has not yet been finalized); and
  
  - Failure to comply with the HIPAA Security Standards (including appointing a security official and completing a security risk assessment).

Business associates remain contractually liable for other requirements of the BAA. The Preamble clarifies that business associates are not required to provide a privacy notice or designate a privacy official unless otherwise agreed to in the BAA.
Practical Observation: This is a very big change for many business associates. Now business associates will need to conduct their own security risk assessment and implement their own HIPAA privacy and security procedures and training. In addition, business associates will be required to have a BAA in place with their subcontractors (who in turn must have BAAAs in place with their subcontractors). While many business associates may be prepared to comply with these requirements, their subcontractors may not be. In addition, both plans and business associates will need to take inventory of their vendors to determine whether additional BAAs need to be added based on the new guidance regarding who is a business associate (particularly if a vendor had been relying on the conduit exception before, which HHS is reading more narrowly now).

- **Covered Entity May Be Liable for Business Associate’s Actions** – Under the current rule, a covered entity only would be liable for a business associate’s actions if it knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate’s obligations. The new rules instead make the covered entity liable for the acts of business associates who are “agents” (and the business associate liable for acts of subcontractors who are “agents”) under the federal common law of agency, where the business associate or subcontractor is acting within their scope as agent. The Preamble says that an analysis of whether a business associate is an agent will be fact specific, taking into account the terms of the BAA as well as the totality of the circumstances. HHS notes that labels given to the parties do not necessarily control whether an agency relationship exists. Rather, the Preamble says that the essential factor in determining whether an agency relationship exists is the “right or authority of the covered entity to control the business associate’s conduct in the course of performing a service on behalf of the covered entity.” The Preamble provides an example where the BAA says that a business associate must mail PHI available based on the instructions to be provided or under direction of the covered entity and says that this type of provision would create an agency relationship because the covered entity has a right to give interim instruction and direction during the course of the relationship.

Practical Observation: Adopting the common law of agency as the basis for determining whether a covered entity is liable for a business associate’s acts definitely muddies the waters for covered entities trying to delegate functions while minimizing HIPAA liability. Many BAAs intentionally allow flexibility to have the covered entity direct the business associate when a need arises (for example, the business associate must provide individual access at the direction of the covered entity). It is not clear whether simply retaining this type of control would cause the business associate to be considered an “agent.” Covered entities should review their BAAs and underlying service agreements to determine how much control they retain and whether they are willing to risk potentially having their business associate be considered an agent, exposing the covered entity to more liability.

**II. RIGHT TO ACCESS PHI**

**Pre-HITECH:**

Participants may request access to their PHI, and the plan generally has to respond within 30 days (60 days where the information is maintained off-site), plus a 30-day extension. The covered entity is required to allow access either by inspection or by providing copies, as requested by the individual.

**What’s New:**

- **Disclosure in Electronic Form** - These requirements continue to apply, but under the new rules, if the information is maintained electronically, the individual has a right to request the information in electronic form. The plan...
must provide the information in the form and format requested by the individual within 30 days (plus a 30-day extension) if the information is "readily producible" - for example, in Word, Excel, text, or HTML. If not readily producible, the plan must provide in a readable electronic form as agreed to by the parties. In any event, a plan cannot deny providing the information electronically, and the Preamble to the rules suggests that the plan at least be able to provide the information in PDF form. The Preamble also notes that if the information includes electronic links or attachments, this information also must be included in the electronic copy. The plan is permitted to charge for labor and supplies, such as where an individual requests that electronic information be provided on portable media like a flash drive.

- **Request to Forward to Third Party** - The rules also state that an individual is permitted to designate a third party to receive the information, and the plan must comply. The rule requires that the designation must be in writing, clearly designate the third party, and be signed by the individual. The Preamble clarifies that an individual can request that the information be emailed to him or her, even in non-encrypted form.

Practical Observation: *Health plans will need to update their HIPAA Privacy Procedures to accommodate this new individual right to request their PHI in electronic form. Plans also should reach out to business associates who may hold this information (it does not appear that the 60-day offsite rule extends to electronic information). Plans should think about what mechanisms they will use to provide information electronically ahead of time, since the 30-day clock will start running upon the participant’s request. In addition, plans may need to reassess how electronic PHI is stored so that it can be produced quickly and update their HIPAA privacy training so workforce members are aware of how to respond to this new rule.*

III. **RIGHT TO RESTRICT DISCLOSURES OF PHI**

**Pre-HITECH:**

Under the current rule, an individual has a right to request that the covered entity restrict disclosures of PHI, even for the purposes of treatment, payment, or health care operations. However, the covered entity was not required to agree to the restriction, and, as a practical matter, many did not since tracking these restrictions could be administratively difficult.

**What's New:**

- **Must Restrict Disclosure Where Individual Paid Cost Himself or Herself** - The new rule requires the covered entity to agree to the restriction where the disclosure would be to a health plan for payment or health care operations purposes and the individual has paid out of pocket in full for the service. The Preamble notes that covered entities will need to use some method to flag PHI that has been restricted. However, providers are not required to notify "downstream providers" of the restriction. Rather, it is the individual's obligation to request restrictions from subsequent providers.

- **Bundled Services** - Regarding services that are "bundled" and for which an individual only has paid out of pocket for some services, the provider must restrict disclosure of the services for which the individual has paid out of pocket if possible. If not, the provider should counsel the individual about which services will be disclosed and give the individual an opportunity to pay out of pocket for all services in the bundle.
• **Application to Health Plans** - The rule applies to covered entities disclosing PHI to a health plan, which most likely will include disclosures by providers to health plans, but technically could include disclosures from one health plan to another health plan. The Preamble notes that the rule, "in effect, will apply only to covered health care providers," and all examples HHS provides relate to providers. The Preamble also says that only providers are required to include this additional right to restrict information in their Notice of Privacy Practices.

More likely, health plans will be indirectly impacted by possibly having gaps in their claims information. The Preamble does clarify that if an individual pays out of pocket and requests a restriction for a service, but does not pay out of pocket for follow-up care, the provider may need to include information about the initial care that was previously restricted in order to have the service deemed medically necessary. The Preamble encourages the provider to have an "open dialogue" with the individual to ensure they are aware that prior information may need to be disclosed unless the individual pays out of pocket for the follow-up service.

• **Application to HMOs** - If a provider within an HMO is restricted by law from accepting out of pocket payments from individuals, the Preamble says that the provider may counsel the individual that he or she may need to use an out-of-network provider in order to restrict disclosure. However, the Preamble notes that a contractual requirement that the HMO provider submit all claims to the HMO would not be considered "required by law," and in that case, the provider must comply. The Preamble says that HMO providers may need to update their contracts with the HMO in the interim time until the requirement applies - 9/23/13.

• **Application to FSAs & HSAs** - If an individual pays for services with funds from a Flexible Spending Account (FSA) or Health Savings Account (HSA), the individual still will be considered to have paid out of pocket, so still has a right to request a restriction on disclosures of PHI related to the service. However, the individual may not restrict disclosures to the FSA or HSA where necessary to effectuate payment. This new provision would not apply to health reimbursement arrangements (HRAs) because HRAs are funded by the employer.

---

**Practical Observation:** Health plans technically may have to comply with this requirement if requested within 30 days so should include in their privacy procedures - at least to review on a case-by-case basis if there is a request. As noted above, the Preamble states that health plans do not need to revise their Notices of Privacy Practices for this requirement (only providers). Regarding potential "gaps" in claims information from providers where there is a restriction in place, plans simply will have to decide claims based on the information in front of them. If a follow-up or related claim is denied, such as due to lack of information or medical necessity, the provider must decide whether to disclose previously restricted information when submitting the new claim.

---

**IV. SECURITY BREACH NOTIFICATIONS**

**Interim Final Rule:**

Starting 9/23/09, if a health plan experienced a "breach" of its PHI, it has been required to notify individuals, HHS, and, in some cases, the media. The interim final rule defines a “breach” as an unauthorized use or disclosure that poses “significant risk of financial, reputational, or other harm to the individual.” HHS said that factors to consider include to whom the information was disclosed, the type of information, and what steps were taken upon discovery of the use or disclosure. In addition, information that has been encrypted or destroyed pursuant to certain technical notices is considered under a safe harbor and protected from the breach rules.
The interim final rule provides three exceptions of impermissible uses that are not considered “breaches”: (1) where there has been unintentional access by a covered entity or business associate’s employee in the scope and course of employment that does not result in further disclosure; (2) inadvertent disclosure from one covered entity or business associate employee to a similarly situated employee who also is authorized to access the information, and (3) where the recipient would not reasonably have been able to retain the information, such as if an envelope was returned unopened. The interim final rule also allows an exception with respect to disclosure of certain limited data set information.

Generally, the interim final rule requires the plan to notify the individual within 60 days after discovering a breach and lists content that must be included in the notice. The plan must notify HHS immediately if the breach involves 500 or more people and, for smaller breaches, must keep a list of breaches and file a “breach log” annually by March 1st. The plan must notify the media if the breach involves more than 500 residents in a state.

What’s New:

- **Burden on Plan / Harm Threshold Replaced with “Compromised” Standard** - Under the new rules, a “breach” is an acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA privacy and security rules that “compromises” the security or privacy of the PHI. HHS said that some had interpreted the “harm threshold” in the interim final rule as setting a higher threshold for breach notification than HHS had intended. HHS said that this change was to clarify its position that a breach notification is necessary in all situations except those in which the covered entity or business associate demonstrates that there is a “low probability” that the PHI has been “compromised.” The Preamble states that the burden is on the covered entity or business associate to demonstrate that either an impermissible use did not constitute a breach or that the proper notifications were made. The Preamble says that the plan must conduct a risk assessment to make this determination and must maintain documentation sufficient to meet the burden of proof. The Preamble also states that a violation of the “minimum necessary” rule under HIPAA could be considered a breach.

- **Factors To Consider** – The new rules provide that the plan’s risk assessment must include at least the following factors: (i) the nature and extent of the PHI involved; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which risk has been mitigated. The Preamble provides an example where a covered entity misdirects a fax containing PHI to the wrong physician practice. Upon receipt, the physician calls the covered entity to say he has received the fax in error and destroyed it. The Preamble says that, after a risk assessment considering the above factors, a covered entity may determine there was a low probability of the information being compromised, so there would be no breach notification requirement.

Practical Observation: HHS clearly intends the new “compromised” standard to result in more impermissible uses and disclosures being considered “breaches” that require the necessary notification. However, the new rules do still have factors that the plan must consider in a risk assessment that are very similar to the factors in the interim final rule. Not every HIPAA violation should necessarily be considered a breach. And given the fact that HHS often uses notifications of these breaches as the basis to launch investigations and penalties, plans should take the time to carefully consider the facts and the guidance provided in the Preamble with respect to factors, examples, and issues to consider. The burden is on the plan to show that an impermissible use or disclosure is not a breach, so plans should be sure to carefully document their decision, information considered, rationale, and any mitigating actions. Plans should retain this documentation in case of audit or questions by HHS.
• **Exceptions** – Generally, the exceptions to the rule (listed above under “Interim Final Rule”) remain the same. However, the new rules remove the exception for limited data sets that do not contain dates of birth or zip codes. Under the new rule, if there is an impermissible disclosure from such a limited data set, the plan must conduct a risk assessment under the normal rules. The safe harbor for encrypted and destroyed information (when performed under the adopted technical notices) remains.

• **Specific Notification Requirements** – The content required to be included in a notification is the same as in the interim final rule, along with the timeframes and parameters for providing notifications to individuals, HHS, and the media. The Preamble did clarify that one notification could be sent to a participant and spouse or other dependents residing at the same address and that an electronic notice could be provided where the individual “affirmatively” agrees.

• **Business Associates** – The new rules require that the BAA address the security breach rules and adopt the prior requirement that business associate notify the covered entity within 60 days of discovery of the breach and then the covered entity has 60 days to make the required notifications. The final rule also adopts the exception where the business associate is acting as an “agent” for the covered entity, in which case the two are treated as one entity, and the covered entity must make the required notifications within 60 days of the business associate’s discovery. The Preamble says that whether a business associate is considered an “agent” will be based on facts and circumstances, taking into account federal common law and the covered entity’s ability to control the business associate’s actions. The Preamble also notes that if the covered entity and business associate disagree as to whether a disclosure is a “breach,” the burden is ultimately on the covered entity to show that there was low probability of the information being compromised.

**Practical Observation:** Many plans want to delegate notice obligations to their business associates, particularly where the breach was on the part of the business associate. However, the Preamble clarifies that it is the covered entity that ultimately has this obligation (and ensuing penalties for failure to provide). Covered entities should be clear in their BAAs which party makes the determination about what is a “breach,” which party provides notifications to individuals, HHS, and the media, and which party is responsible for payment of any related costs. In addition, both the business associate and covered entity may want to retain the right to approve the content of any notification that includes their names. While a health plan may want to delegate delivery of the notifications to the business associate, they still may want to “frame the message” that potentially could go out to thousands of participants, the media, and HHS (or at least be prepared for questions).

**V. USING PHI FOR MARKETING PURPOSES / SALE OF PHI**

**Pre-HITECH:**

The privacy rules required that a covered entity obtain individual authorization for using PHI to make communications for marketing purposes and define ”marketing” to mean communications that encourage the recipient to purchase or use a product or service. The prior rules have several exceptions, including face-to-face communications, gifts of nominal value, or communications to describe health-related products or services included in a plan of benefits or available only to health plan enrollees that add value to, but are not part of, a plan of benefits. The marketing definition also includes exceptions for communications about replacements and enhancements to a health plan, case management or care coordination, or to direct or recommend alternative treatments, providers, or settings of care.
What's New:

- **If Remuneration Involved, Will Be Marketing** - The new rules largely retain the exceptions to the marketing definition listed above, but add that if the health plan receives "financial remuneration" in exchange for the communication, the communication will be considered marketing and only may be made if authorized by the individual. The authorization must expressly state that remuneration is involved, but the Preamble notes that the authorization is not required to be limited to a single product or service. Rather, the authorization may be more open-ended to "apply to subsidized communications generally."

- **What is Financial Remuneration?** - The rules define "financial remuneration" as direct or indirect payment from or on behalf of a third party whose product or service is being described. The Preamble clarifies that financial remuneration only includes financial payments made in exchange for making the communication and not "in kind" benefits. In addition, in order to trigger the authorization requirement, the purpose of the communication must be to promote the third party's product or services. If a third party provides financial remuneration to a health plan to implement a disease management program, the plan could send communications about the disease management program without authorization because the plan would be promoting its own program, rather than the third party's program.

Practical Observation - The new rules essentially require authorization where the health plan receives direct or indirect payment from the third party whose product is being "pitched." Many plans use PHI to send communications about alternative drugs, wellness programs, or other health insurance products, but do not receive payment from the party whose product or service is being promoted. These communications generally would be allowed to continue, assuming they otherwise fall under the other elements of the marketing exception. Where a plan thinks it may receive remuneration, it may be wise to go ahead and build this language into an authorization that allows an individual to "opt in" to these types of communications at enrollment. Sometimes these communications provide information on discounts or free services, so may be valuable to the participant (and the plan can point out the merits of these communications when seeking authorization).

- **Exception for Face-to-Face Communications / Nominal Gifts** - The final rule retains the exceptions for face-to-face communications, but HHS notes that email or phone communications would fall under the general rule above. The final rule also retains the exception related to gifts of nominal value.

- **Exception for Communications About Current Drugs** - In addition, the final rules add an exception allowing refill reminders or other communications about a drug or biologic currently prescribed for an individual, even if the covered entity receives financial remuneration from the third party (e.g., pharmaceutical company). The Preamble provides that this exception would include communications about generic equivalents of drugs an individual is prescribed, adherence communications, and communications about all aspects of the drug delivery system, such as information about insulin pumps. The remuneration must be reasonably related to the cost of making the communication, which HHS says includes only the cost of labor, supplies, and postage to make the communication. The Preamble provides an example where a drug manufacturer provides financial remuneration to a pharmacy to provide refill reminders. The example says that this type of communication would be permitted without authorization as long as the remuneration only covers the cost to draft, print, and mail the communication. However, if the drug manufacturer provides an additional financial incentive, the pharmacy must obtain authorization - unless the communication is given to the individual as part of a face-to-face communication (under the exception described above).
• **Other Exceptions** - The Preamble also clarifies that the marketing restriction does not apply to communications to promote health in general that does not promote a product or service, such as annual mammogram reminders. In addition, HHS says that the restrictions do not apply to communications about government-sponsored programs, such as Medicare or Medicaid, because there is no "commercial component."

• **Sale of PHI** - Separately, the new rules also require authorization if the plan sells PHI. The authorization must state that the disclosure involves remuneration. The regulations define "sale" of PHI to include where the plan directly or indirectly receives remuneration from the recipient of the PHI. The Preamble makes clear that, unlike marketing, remuneration here includes financial or nonfinancial (i.e., in-kind) benefits and provides an example where a third party offers a covered entity computers in exchange for disclosing PHI (even for a permitted reason) but then allows the covered entity to use the computers for other reasons or to retain after the allowed disclosures have been made. The Preamble clarifies that the limitation on sale of PHI does not apply to exchange of remuneration to business associates performing a plan function or to disclosures within single legal entity or among affiliated covered entities - only outside the entity.

**Practical Observation:** The prohibition on the sale of PHI likely will impact providers and researchers the most. However, plans should consider this rule when entering into agreements with third parties, including TPAs, where the third party retains PHI or is able to use PHI for an additional purpose, such as to create a database and where the plan arguably has received some type of remuneration, such as a fee concession or additional zero-cost benefit add-on like a wellness program, to collect the information. Not only might this type of disclosure violate the business associate agreement (or not be considered treatment, payment, or health care operations in the first place), but now could be considered sale of PHI for which the plan would need authorization. (Plans could avoid this issue by carefully considering how business associates or other third parties will use plan data or only allowing business associates to retain or use de-identified information.

VI. **DISCLOSURE OF DECEASED INDIVIDUAL’S INFORMATION TO FAMILY MEMBERS**

**Pre-HITECH:**

The current rules allow a covered entity to disclose to a family member, other relative, or close personal friend of the individual, or any other person identified by the individual, the PHI "directly relevant" to such person's involvement with the individual's care or payment for health care. The rule states that, where the individual is present and has the capacity to make decisions, the covered entity only may disclose PHI if the individual does not object or the covered entity reasonably infers from the circumstances, based on professional judgment, that the individual does not object. If the individual is not present or is incapacitated, the covered entity may disclose PHI if, in the exercise of professional judgment, it determines the disclosure is in the "best interest" of the individual.

**What's New:**

• **Disclosure to Family Members & Others Involved in Care** - The new rules extend this provision to deceased individuals and allows a plan to disclose a decedent's PHI to a family member or others who were involved in the care or payment for care prior to death, unless doing so is "inconsistent with any prior expressed preference of the individual that is known" to the plan. The Preamble expressly states that this group could include spouse, parents, children, domestic partners, other relatives, or friends of a decedent. The Preamble clarifies that the information provided must be limited to information that is relevant to the person's involvement and provides an example where a provider may disclose billing information to a family member assisting with the estate, but
could not share information about past, unrelated medical problems. The Preamble says that, in some cases, it will be readily apparent that a family member or other person has been involved in the individual’s care, such as someone having been identified by the decedent or someone who has made prior inquiries. In other cases, the covered entity needs to “just have reasonable assurance” that the person is a family member or other person involved in the individual’s care or payment for care. The Preamble says, for example, the person may indicate how they are related to the decedent or other sufficient details about the decedent’s circumstances to indicate involvement.

- **No Longer PHI After 50 Years** - The new rules also provide that information no longer will be considered PHI once the individual has been deceased for 50 years.

**Practical Observation**: Most health plans retain health information for the time period prescribed by HIPAA and ERISA (generally 6 years), so the rule "de-identifying" PHI for a deceased individual after 50 years likely will have little impact. More important to health plans is the provision clarifying when a health plan may disclose PHI to a family member or other third party after a participant’s death. The Preamble discussion around this new provision can be helpful for health plans determining when it is appropriate to disclose PHI to family members even when someone is alive.

### VII. GENETIC INFORMATION / OVERLAP WITH GINA

**Pre-HITECH:**

In 2008, Congress passed the Genetic Information Nondiscrimination Act (GINA), which generally prohibits a group health plan or health insurance issuer from performing underwriting activities based on genetic information. For example, a health plan could not set group or individual premiums based on the genetic information of participants. HHS, DOL, and IRS issued regulations under GINA, which further prohibited a health plan from requesting genetic information (e.g., family history) as part of enrollment or providing any type of reward to provide genetic information. For example, a health plan no longer could provide a reward to a participant to complete a health risk assessment that included family history.

**What's New:**

- **Genetic Information is PHI** - The new rules clarify that genetic information is PHI (this is not really new - plans likely considered this information to be PHI all along).

- **GINA Violations Are Now HIPAA Violations** - The new rules prohibit a health plan from “underwriting” based on genetic information and adopt the definition of “underwriting” from Title I of GINA and its implementing regulations. This means that a violation of the GINA underwriting rules will now be a HIPAA privacy violation. The Preamble provides two examples of prohibited types of underwriting: where an insurer uses family medical history or results from genetic tests to adjust the plan’s aggregate premium or where a group health plan grants a premium reduction to an individual based on collection of family medical history on a health risk assessment.
Practical Observation - By incorporating GINA into the privacy rules and expressly prohibiting underwriting based on genetic information, it appears that if a health plan violates GINA, it not only has to worry about GINA violations, but also the (much greater) HIPAA privacy penalties as well. Health plans that have wellness programs or health risk assessments that collect or base eligibility on family history (including a spouse) should be extra cautious and review these programs since the stakes appear to be much higher now.

- Expansion of Entities Subject to GINA to Include HIPAA Exempted Benefits (Except Long-Term Care) – Currently, GINA applies to group health plans under the HIPAA portability rule, but does not apply to HIPAA exempted benefits, such as limited scope dental and vision, supplemental plans, disease only plans, fixed indemnity coverage, and long-term care coverage. The HIPAA privacy rules (even the current rules) do not adopt all of HIPAA’s exempted benefits, so the above listed plans that may be excepted from the HIPAA portability rules are subject to the HIPAA privacy rules. The new final privacy rules, which prohibit underwriting based on genetic information, extend this prohibition to all covered entity health plans, except long-term care. This means that HIPAA exempted benefits that do not currently have to comply with GINA will be subject not only to the confidentiality provisions of the HIPAA privacy rules but also several of the prohibitions found in the GINA statute. The Preamble says that HHS did not extend this liability to long-term care coverage because it simply did not have enough information about whether prohibiting underwriting based on genetic information would impact this industry, but it will reassess as it receives more information. The Preamble also clarifies that the extension of GINA’s underwriting rules does not apply to covered entity health care providers.

- Notice of Privacy Practices - The new rules require health plans that perform underwriting to include a statement in their HIPAA Privacy Notices that they are prohibited from using or disclosing genetic information for such purposes (except for long-term care issuers).

Practical Observation – This is a potentially significant development for HIPAA exempted benefits, for which plans and issuers have not had to consider GINA’s prohibitions before. Issuers of exempted benefits will need to review how they collect and use any family history or genetic information to ensure that they do not violate GINA’s underwriting rules, which now could lead to HIPAA privacy penalties. In addition, issuers of long-term care coverage may want to offer input to HHS regarding how this type of provision would impact them and keep this provision on their radars for possible future changes.

VIII. UPDATES TO HIPAA PRIVACY NOTICE

Pre-HITECH:

The current privacy rules require health plans to provide a privacy notice to new enrollees and within 60 days of any material changes. The plan must provide a notification every 3 years instructing participants as to how to request the full privacy notice. The prior regulations set out the content requirements for the notice.

What’s New:

- Updated Content - The new rules require that the privacy notice be updated to include the following:
  - A description of the types of uses and disclosures that require an authorization, including when related to psychotherapy notes (where applicable for that covered entity), for marketing purposes, or related to the sale of PHI;

This publication is provided for educational and informational purposes only and does not contain legal advice. The information should in no way be taken as an indication of future legal results. Accordingly, you should not act on any information provided without consulting legal counsel. To comply with U.S. Treasury Regulations, we also inform you that, unless expressly stated otherwise, any tax advice contained in this communication is not intended to be used and cannot be used by any taxpayer to avoid penalties under the Internal Revenue Code, and such advice cannot be quoted or referenced to promote or market to another party any transaction or matter addressed in this communication.
- A statement that other uses and disclosures not described in the notice will be made only with the individual’s written authorization, which the individual may revoke;

- Where a covered entity intends to engage in fundraising activities, that the individual has a right to opt out of receiving such communications;

- Where a covered entity (except a long-term care issuer) intends to use or disclose PHI for underwriting purposes, a statement that the covered entity is prohibited from using or disclosing genetic information for such purposes;

- A statement that a covered entity is not required to agree to a requested restriction on disclosures of PHI to a health plan where the individual has paid out of pocket in full for the service (the Preamble notes that this requirement only applies to health care providers); and

- A statement that the covered entity will notify affected individuals following a breach of unsecured PHI.

- Due Dates for Delivery - The Preamble provides two rules regarding delivery of the new, updated notice, depending on whether the plan posts its notice on its website:

  - If the plan posts its current privacy notice on its website, it must update that online notice by 9/23/13 and then deliver notices to individuals as part of its next annual mailing.

  - If the plan does not post its current privacy notice on its website, it must deliver notices to individuals within 60 days of the required 9/23/13 applicability date (or 11/23/13).

This publication is provided for educational and informational purposes only and does not contain legal advice. The information should in no way be taken as an indication of future legal results. Accordingly, you should not act on any information provided without consulting legal counsel. To comply with U.S. Treasury Regulations, we also inform you that, unless expressly stated otherwise, any tax advice contained in this communication is not intended to be used and cannot be used by any taxpayer to avoid penalties under the Internal Revenue Code, and such advice cannot be quoted or referenced to promote or market to another party any transaction or matter addressed in this communication.
beginning on the first date the covered entity or business associate knew, or by exercising reasonable diligence, would have known that the violation occurred. Factors to determine the penalty amount include the nature and extent of the violation; the physical, financial, or reputational harm resulting from the violation; history of prior compliance (or violations) by the covered entity or business associate; and the financial condition of the covered entity or business associate that may impact its ability to comply. The final rule also expressly allows the Secretary to coordinate with other law enforcement agencies, such as State Attorneys General or the FTC in pursuing remedies available to these parties.

- **Willful Neglect** – Where a violation may involve “willful neglect,” the new rules remove some of the Secretary’s discretion and require the Secretary to investigate. The regulations define “willful neglect” to mean conscious, intentional failure or reckless indifference to the obligation to comply. The new rules provide that the Secretary “will” investigate a complaint when a preliminary review of the facts indicates a “possible” violation due to willful neglect. The Secretary “may” investigate other complaints. The Secretary still has authority to attempt to reach a resolution through “informal means,” which may include a covered entity demonstrating compliance or completing a corrective action plan, but the Secretary is not required to use informal means when the violation is due to willful neglect and may issue a penalty instead.

**Practical Observation** - We have seen stepped up enforcement by HHS, with penalties being assessed against both health care providers and health plans - large and small - in some cases for violations that appeared to be inadvertent errors. HHS investigations have been triggered by individual complaints, breach notifications to HHS, and a new audit program implemented by HHS, as mandated by the HITECH Act. The final rules allow the Secretary to share information with other law enforcement agencies, such as State Attorneys General, which likely will expand investigation and enforcement even more. Covered entities should do what they can to mitigate this risk, such as reviewing HIPAA privacy procedures, performing HIPAA security assessments, renewing HIPAA training, and ensuring that their BAAs are updated and protect them against additional liability.

**X. OTHER CHANGES**

- **Other Individual Rights** – The new rules did not change the provisions related to an individual’s right to amend PHI, request confidential communications, or request an accounting of certain PHI disclosures. Note that HHS issued proposed accounting rules in May 2011, which would have required covered entities, including business associates, to keep a log of anyone who accessed electronic PHI and provide an access report to individuals upon request. This would be a significant new requirement that even HHS recognized goes beyond the requirements of the HITECH Act. This will be an area to watch.

- **Student Immunization Information** – The new rules revise the exception for disclosures for public health activities to allow a covered entity to disclose immunization information to a school where state or other law requires the school to have such information prior to a student’s admission, provided the information is limited to proof of immunization. The covered entity still will be required to document and obtain some type of agreement from the parent or guardian (or individual if an adult or emancipated minor). The Preamble says that this agreement must be affirmative (rather than an opt out or negative election), but the agreement may be oral.
• **Fundraising Communications** – The new rules allow a covered entity to use or disclose the following PHI with respect to its own fundraising purposes, such as a hospital sending targeted fundraising invitations to former patients: names and contact information, date of birth, dates of care, department of service, treating physician, outcome information, and health insurance status. The covered entity may use or disclose this information only if each fundraising communication provides a clear and conspicuous opportunity for the recipient to elect not to receive further fundraising communications. This notice also must appear in the Notice of Privacy Practices.

• **Hybrid Entity Rules** – A hybrid entity is an entity that includes both health care and non-health care components, such as an insurer that provides both medical and disability policies. The current rules allow such an entity to designate its health care components and limit HIPAA applicability to those health care components. However, where a covered entity has made these designations, it must have some type of “firewall” between health and non-health components and treat disclosures from a health care component to a non-health care component as a disclosure to a third party. In some cases, this could include business associate functions that the covered entity is providing to itself, such as a company providing TPA services to its own health plan. The new rules require that a health care component of a hybrid entity include all business associate functions within the entity.

* * *

Every health plan, health insurer, and third party administrator will need to make at least some changes in order to comply with these rules. Time is short for compliance of some of these items, so health plans should start reviewing what changes are needed now.