January 29, 2013

Final HIPAA Rule Has Sweeping Impact on Covered Entities and Business Associates

By Megan Hardiman, Michael Callahan, Russell Greenblatt, Christopher Buch, Stephanie Goldman and Sarah Sager

Executive Summary

On January 25, 2013, the Department of Health and Human Services (HHS) published the highly anticipated Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule (the "Final Rule"). The Final Rule represents a material development in the area of health care privacy, and has important operational consequences for covered entities and business associates. Major changes include the following:

- **Final Rule Requires Changes in Breach Notice Policies; Likely to Increase Breach Reporting.** The Final Rule eliminates the "significant risk of harm" threshold for breach notification. Under the Final Rule, any impermissible use or disclosure of protected health information (PHI) is presumed to be a breach requiring notification, unless the covered entity or business associate demonstrates through a risk assessment that there is a "low probability that the PHI has been compromised" or unless an exception applies. The Final Rule requires entities to consider at least four "objective" factors in conducting their risk assessments. These changes are likely to increase breach notifications. As a result, affected entities should make a concerted effort to encrypt PHI, since HIPAA breach notification requirements do not apply to PHI that has been encrypted in accordance with HHS guidance. In addition, breach notification policies, procedures and protocols will need to be revised.
- **Significant Impact on Business Associates; Business Associate Agreements Need to Be Revised.** The Final Rule implements numerous changes extending direct liability for HIPAA compliance to business associates, and affirms that covered entities and business associates are generally liable for acts of business associate "agents." It also expands the definition of business associates. Among other things, the revised definition treats certain subcontractors of the business associate as direct business associates, with all the same compliance obligations and liability exposures. The Final Rule also modifies the requirements for the content of business associate agreements. As a result, business associates need to ensure they have effective HIPAA compliance programs in place. Furthermore, business associates and covered entities generally will need to revise business associate agreement forms and renegotiate existing business associate agreements (subject to the grandfathering provisions noted below, which extend the deadline to September 23, 2014, for certain existing agreements). HHS has posted a sample revised business associate agreement (available here). However, covered entities and business associates generally will want to incorporate additional protections not included in the HHS form.
- **Numerous Privacy Rule Changes Will Impact Operations, Forms, Policies and Procedures.** Key changes include: establishing stronger limits on marketing; increasing flexibility for fundraising; implementing rules that prohibit sales of PHI; permitting authorizations for future research and providing flexibility on compound research authorizations; providing for expiration of HIPAA Privacy Rule protections 50 years after an individual's death; giving greater flexibility as to disclosures to a decedent's family members and others who were involved in the decedent's care or payment for care prior to death; modifying the Notices of Privacy Practice (NPP) contents and providing new rules on redistribution requirements; adopting provisions implementing an individual's right to restrict certain disclosures of PHI to a health plan; and implementing rules to enhance a patient's right to access electronic copies of PHI. These changes will have a significant impact on policies, procedures and forms, including the NPP.

- **Genetic Information Nondiscrimination Act of 2008 (GINA) Modifications.** The Final Rule generally prohibits covered entity health plans from using or disclosing genetic information for underwriting purposes. Covered entity health plans subject to the prohibition will need to revise their NPPs accordingly.
- **Enhanced Enforcement Is Here to Stay.** To implement the Health Information Technology for Economic and Clinical Health (HITECH) Act, HHS previously issued an interim final enforcement rule establishing four categories of violations for covered entities and business associates, with increasing penalty amounts reflecting increased levels of culpability, and a maximum penalty amount of $1.5 million annually for all violations of an identical provision. The Final Rule retains this penalty structure and makes other changes to strengthen enforcement. Now that the Final Rule has provided long-awaited definitive guidance to the industry on key HITECH Act changes, covered entities and business associates can expect to see enhanced enforcement follow.

180-Day Compliance Deadline for Implementing Most Changes. The Final Rule goes into effect on March 26, 2013, and has a general compliance deadline of September 23, 2013. As noted below, business associate agreements in existence prior to January 25, 2013, generally qualify for a longer transition period for modifications. HHS estimates total implementation costs for affected entities at $114 million to $225.4 million for the first year of implementation, and approximately $14.5 million each year thereafter.

Compliance Action Steps

Covered entities and business associates will need to act now to ensure compliance by the compliance deadline. Recommended steps include:

- **GAP Analysis.** Assess existing policies and procedures for compliance gaps.
- **Policy/Procedure Revisions.** Numerous policies and procedures will need to be revised to incorporate these changes in law.
- **Business Associate Agreement Modifications.** Covered entities and business associates need to review and update their form of business associate agreement, and identify a plan for transitioning existing agreements onto that form.
- **Notice of Privacy Practices; Distribution.** NPPs need to be reviewed and updated as necessary. Covered entities must identify and develop a plan for meeting applicable distribution requirements.
- **Other Forms.** Other forms, such as requests for access, may need to be created or updated.
- **Training.** Covered entities and business associates will need to train workforce on the new requirements.
- **Encryption.** In light of the changes to the breach notice rule, it makes good sense to re-double efforts to take advantage of the "safe harbor" protection that encrypting PHI provides against the need to give costly HIPAA breach notifications.

A detailed summary of key changes follows. Due to the length of the Final Rule (almost 600 pages), these changes are divided by major topic, to allow the reader to readily find those of most interest.

I. Key Breach Notification Changes

Removal of Harm Standard and Modification of Risk Assessment. The Final Rule makes a number of significant changes that are likely to increase breach notification, thereby placing a premium on encrypting PHI as a means of avoiding costly HIPAA breach notification altogether. Under current rules, a breach of unsecured PHI must be reported only if it poses "a significant risk of financial, reputational, or other harm to an individual." The Final Rule eliminates the "significant risk of harm" threshold. Under the Final Rule, any impermissible use or disclosure of PHI is presumed to be a breach requiring notification, unless the covered entity or business associate demonstrates through a risk assessment that there is a "low probability that the PHI has been compromised" or that one of the Rule's narrow exceptions applies. Under the Final Rule, a risk assessment must consider at least the following four "objective" factors. However, HHS notes that it may also be appropriate to consider other factors, depending on the circumstances.

1. **Nature and Extent of PHI.** The first factor requires covered entities and business associates to evaluate the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
    - **Example**: If a covered entity impermissibly disclosed a list of patient names, addresses and hospital identification numbers, the PHI is obviously identifiable, and a risk assessment likely would determine that there is more than a low probability that the information has been compromised, dependent on an assessment of the other factors discussed below. In contrast, if the covered entity disclosed a list of patient discharge dates and diagnoses, the entity would need to consider whether any of the individuals could be identified based on the specificity of the diagnosis, the size of the community served by the covered entity, or whether the unauthorized recipient of the information may have the ability to combine the information with other available information to re-identify the affected individuals (considering this factor in combination with the second factor discussed below).
    - The entity must evaluate all the factors, including those discussed below, before making a determination about the probability of risk that the PHI has been compromised.
2. **Nature of the Recipient.** The second factor requires covered entities and business associates to consider the unauthorized person who used the PHI or to whom the disclosure was made.
    - Where PHI is disclosed to another covered entity or business associate, there may be a lower probability that the PHI has been compromised because the recipient of the information is obligated by HIPAA to protect the privacy and security of the information in a similar manner as the disclosing entity.
    - If the information impermissibly used or disclosed is not immediately identifiable, entities should determine whether the unauthorized person who received the PHI has the ability to re-identify the information.
    - **Example:** If information containing dates of health care service and diagnoses of certain employees was impermissibly disclosed to their employer, the employer may be able to determine that the information pertains to specific employees based on other information available to the employer, such as dates of absence from work. In this case, there may be more than a low probability that the PHI has been compromised.
3. **Was PHI Actually Acquired/Viewed?** The third factor requires covered entities and business associates to investigate whether the PHI was actually acquired or viewed, or, alternatively, if only the opportunity existed for the information to be acquired or viewed.
    - **Example:** If a laptop computer was stolen and later recovered and a forensic analysis shows that the PHI on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised, the entity could determine that the information was not actually acquired by an unauthorized individual even though the opportunity existed. In contrast, if a covered entity mailed information to the wrong individual, who opened the envelope and called the entity to say that she received the information in error, the unauthorized recipient clearly viewed and acquired the information.
4. **Mitigation.** The final factor requires covered entities and business associates to consider the extent to which the risk to the PHI has been mitigated.
    - Entities must attempt to mitigate the risks to the PHI following any impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed, and should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised.
    - HHS notes that a covered entity may be able to obtain and rely on the assurances of an employee, affiliated entity, business associate, or another covered entity that the entity or person destroyed information it received in error, while such assurances from certain third parties may not be sufficient.
5. **Other Factors.** A risk assessment will be fact-specific. In a given case, other factors may also need to be considered.

Documentation of Risk Assessments. As under the interim final breach notification rule, covered entities and business associates have the burden of proving that all notices were provided as required, or that the situation was not a breach, and need to maintain relevant documentation (e.g., a thorough risk assessment).

Removal of Limited Data Set Exception to Breach Notification. HHS removed the exception for limited data sets that do not contain any dates of birth and zip codes. Under the Final Rule, an impermissible use or disclosure of a limited data set, even one that does not contain dates of birth and zip codes, will be subject to the same risk assessment process as other breaches. HHS anticipates that this modification will not necessarily affect the outcome in most cases.

- **Clarification on Reporting Newly Discovered Breaches from Prior Years.** Covered entities are required to notify the HHS Secretary of all breaches of unsecured PHI affecting fewer than 500 individuals not later than 60 days after the end of the calendar year in which the breaches were "discovered," and not in which the breaches "occurred." Thus, if a breach of unsecured PHI affecting fewer than 500 individuals that occurred in *a prior year* is "discovered" in *the current calendar year*, the covered entity has until 60 days after the end of the current calendar year in which the breach was discovered to provide notice to the Secretary. HHS emphasizes, however, that this modification does not alter a covered entity's obligation to promptly report the breach to affected individuals without unreasonable delay and no later than 60 calendar days after discovery, and to have in place reasonable and appropriate breach detection systems.
- **Subcontractor Breach Reporting Chain.** HHS clarifies that business associate agreements between business associates and subcontractors must require subcontractors who handle e-PHI to report security incidents and breaches to the business associate. Thus, if a breach of unsecured PHI occurs at a second-tier subcontractor, the subcontractor must notify the business associate subcontractor with which it contracts, which then must notify the business associate which contracts with the covered entity, which must then notify the covered entity of the breach.
- **Breach Reporting Before September 23, 2013.** Until September 23, 2013, covered entities and business associates must continue to comply with the breach notification provisions of the interim final rule on breach notification, which became effective September 23, 2009. Commencing September 23, 2013, the breach notification provisions of this Final Rule apply.

II. Key Changes: Business Associates

The Final Rule expands the definition of business associates, articulates the increased compliance obligations that apply directly to business associates under the HIPAA Rules, and extends direct liability for HIPAA violations to business associates. It also describes the required changes to business associate agreements. Covered entities and business associates generally will need to modify existing business associate agreements. Business associates will also need to ensure they have compliant business associate agreements in place with subcontractors. To the extent they have not already done so, business associates need to ensure they have adopted appropriate HIPAA compliance programs, policies and procedures.

A. An Expanded Definition of "Business Associate"

The Final Rule expands the definition of business associate to generally include a person that creates, receives, *maintains* or transmits PHI on behalf of a covered entity. In addition, the definition of business associate now includes: (1) subcontractors (as described below); (2) health information organizations, e-prescribing gateways and other persons that "provide data transmission services with respect to PHI to a covered entity and that require access on a routine basis to such PHI"; and (3) persons who offer a personal health record to one or more individuals "on behalf of" a covered entity. HHS also adds patient safety activities to the list of functions and activities that gives rise to a business associate relationship in light of the creation of patient safety organizations under the Patient Safety and Quality Improvement Act of 2005.

Inclusion of Subcontractors. Under the Final Rule, a subcontractor is itself a business associate, subject to the same compliance obligations and direct liability under HIPAA as a first-tier business associate. Generally, a subcontractor is defined as a person (other than a business associate workforce member) to whom a business associate delegates a function, activity or service, where the delegated function involves the creation, receipt, maintenance or transmission of PHI.

Business Associate Versus Conduit; Entities That "Maintain" PHI. HHS elaborates in commentary on what it means for a data transmission service to have "access on a routine basis," noting that the "conduit exception" is narrow, and is intended for mere "courier" services. It also notes that the conduit exception is limited to transmission services, including any temporary storage of transmitted data incident to such transmission. In contrast, an entity that *maintains* PHI (whether digital or hard copy) on behalf of a covered entity is a business associate, and not a conduit, even if it does not actually *view*

the information. In HHS's view, the distinguishing factor is the transient versus persistent nature of the entity's opportunity to access PHI. To clarify this point, HHS revised the definition of business associate to include a person who "maintains" PHI on behalf of a covered entity.

More Guidance for Personal Health Record Vendors. HHS commentary provides several additional examples and clarifications regarding when a personal health record vendor is a business associate. Personal health record vendors and covered entities working with such vendors will want to closely review the commentary to the Final Rule.

Business Associate's Disclosure for Own Management and Administration. Disclosures by a business associate for its *own* management and administration or legal responsibilities *do not create a business associate relationship with the recipient*. However, where such disclosures are not required by law, the Final Rule requires that the business associate obtain reasonable assurances the information will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed, and that the person notifies the business associate of any breaches.

B. Business Associate Liability Issues

Direct Liability of Business Associate for Privacy Rule Violations. The HITECH Act did not create direct liability for business associates for compliance with all requirements of the HIPAA Privacy Rule. The Final Rule articulates that business associates are directly liable under the HIPAA Rules for the following:

- Impermissible uses and disclosures (i.e., complying with the terms of the business associate agreement and, generally, not using or disclosing PHI in a manner that would be impermissible if so done by the covered entity; this includes compliance with minimum necessary);
- Failure to provide breach notification to the covered entity;
- Failure to provide access to a copy of electronic PHI to either the covered entity, an individual or such individual's designee;
- Failure to disclose PHI when required by the Secretary to investigate or determine the business associate's compliance with the HIPAA Rules;
- Failure to provide an accounting of disclosures; and
- Failure to comply with the requirements of the HIPAA Security Rule.

Contractual Liability. Business associates remain contractually liable for all other HIPAA Privacy Rule obligations that are included in their contracts or arrangements.

Vicarious Liability for Agent. The Final Rule adopts modifications to provide that a covered entity or business associate is liable for penalties for the failure of its business associate "agent" to perform an obligation on the covered entity's or business associate's behalf. The Final Rule suggests that whether a particular business associate is an "agent" depends on an analysis of the totality of the circumstances, including:

- The time, place and purpose of a business associate agent's conduct;
- Whether a business associate agent engaged in course of conduct subject to a covered entity's control;
- Whether a business associate agent's conduct is commonly done by a business associate to accomplish the service performed on behalf of a covered entity; and
- Whether or not the covered entity reasonably expected that a business associate agent would engage in the conduct in question.

Affected entities will want to carefully review the potentially significant impact of this change.

Non-Compliance by Subcontractors. Furthermore, like in the context of a covered entity's knowledge of non-compliance on the part of its business associate, under the new provisions a business associate that is aware of non-compliance by its subcontractor would be required to take reasonable steps to cure the breach or end the violation and, if such steps were unsuccessful, terminate the contract or arrangement or face liability for non-compliance with the business associate requirements.

C. Business Associate Agreements

The Final Rule continues to require the parties to have in place a written business associate agreement for compliance. The Final Rule also modified the required content of business associate agreements. Specifically, each business associate agreement must require business associates (and subcontractors) to:

- Comply, where applicable, with the HIPAA Security Rule with regard to electronic PHI;
- Report breaches of unsecured PHI to covered entities;
- Ensure that any subcontractors that create or receive PHI on behalf of a business associate agree to the same restrictions and conditions that apply to business associates with respect to such information (subcontractors should be required to execute a *written* business associate agreement evidencing these terms); and
- To the extent the business associate is to carry out a covered entity's obligation under the HIPAA Privacy Rule, comply with the requirements of the HIPAA Privacy Rule that apply to the covered entity in the performance of such obligation.

HHS has posted a sample revised business associate agreement on its website, which may be accessed here. Note that covered entities and business associates will likely wish to incorporate additional protections that are not included in the HHS form.

Whether a person is a business associate is definitional, and is not dependent on the existence of a business associate agreement.

Business Associate Agreements with Subcontractors. A covered entity is *not* required to enter into a written agreement with the subcontractor of the business associate. Rather, this is the obligation of the business associate making the delegation. This requirement to obtain a written business associate agreement extends down the chain indefinitely.

Grandfathering. Recognizing covered entities' and business associates' concerns about the anticipated administrative burden and cost to implement the revised business associate agreement provisions, the Final Rule provides a longer transition period for certain existing agreements, as follows:

- If the parties had a business associate agreement in place prior to January 25, 2013, that complies with the prior provisions of the HIPAA Rules and such agreement is not renewed or modified from March 26, 2013, until September 23, 2013, then the parties can rely on such business associate agreement until the earlier of (i) the date such agreement is renewed or modified, or (ii) September 22, 2014. As of September 23, 2014, the parties must have in place an agreement complying with the Final Rule.
- If the parties did *not* have a compliant business associate agreement in place prior to January 25, 2013, then the parties will need to enter into an agreement complying with the Final Rule by September 23, 2013.

D. Business Associate Security Rule Compliance

To implement the HITECH Act's provisions extending direct liability to business associates for compliance with the Security Rule, the Final Rule made various changes consistent with the proposed rule.

III. Key Modifications to the Privacy Rule

A. Stronger Limits on Marketing

Subsidized Treatment Communications Require Authorization. The Final Rule makes a significant change by requiring authorization for *all* treatment and health care operations communications where the covered entity receives financial remuneration for making the communication from a third party whose product or service is being marketed. The Final Rule opts for a bright line approach of requiring an authorization for *all* subsidized communications that market a health-related product or service, compared to the previously proposed approach that would have allowed a notice-and-opt-out for certain subsidized treatment communications. HHS also eliminated the requirement that existed prior to the Final Rule that a covered entity include in its NPP a statement that the covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual. While this still continues to be accurate for non-subsidized communications, if the communication is subsidized, the individual will be notified via the authorization process.

Financial Remuneration for Marketing: What Counts? For purposes of the marketing provisions, "financial remuneration" means *direct or indirect payment* and does *not* include in-kind or other non-financial benefits. Furthermore, financial remuneration a covered entity receives must be for the purpose of making a communication that encourages individuals to purchase or use *the third party's* product or service. If the financial remuneration is for another purpose, the marketing provision does not apply. Thus, where a third party pays a covered entity to implement a disease management program as part of the covered entity's services, the covered entity could make communications about the program without an authorization, because such communications are not to market the *third party's* product or service.

Contents of Authorizations. Authorizations must disclose the fact that the covered entity receives remuneration. However, an authorization may cover subsidized communications generally (e.g., need not be limited to subsidized communications about a single product or a product of one third party), as long as it adequately describes the intended purposes of the use or disclosure and contains all other required elements.

Face-to-Face/Nominal Gifts. Existing exceptions for "face-to-face" communications and nominal gifts continue to apply.

Refill Reminders/Communications About Currently Prescribed Drugs. The Final Rule adopts the exception for refill reminders and communications about drugs/biologics currently prescribed as proposed. HHS clarifies that costs for which a covered entity may receive remuneration under this exception are costs of necessary labor, supplies and postage. Financial incentives beyond cost are not within the scope of the exception.

Communications Promoting Health in General or About Government Programs. Communications promoting health generally (e.g., promoting annual mammograms), and that do not promote a product or service from a particular provider, do not constitute marketing and thus do not require individual authorization. Also, communications about government-sponsored programs do not fall within the definition of marketing.

B. Sale of PHI

HHS adopts the HITECH Act's prohibition on the sale of protected PHI unless the covered entity or business associate has obtained a valid authorization. HHS defines "sale of protected health information" as "a disclosure of PHI by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI."

Exceptions. Several exceptions to the authorization requirement exist. 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 HIPAA Privacy Rule;
- For disclosures required by law; and
- For any other purpose permitted by and in accordance with the applicable requirements of the HIPAA 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.

HHS provides a number of clarifications about these exceptions, including examples as to the scope of costs that can be included.

"Sale." HHS clarifies that "sale" is not limited to transactions where there is a transfer of ownership of PHI. Thus, sale provisions apply to disclosures in exchange for remuneration including those that result from access, license or lease arrangements.

Effect on Research Grants and Payments. HHS does not consider a sale of PHI to encompass payments to a covered entity in the form of grants, contracts or other arrangements to perform programs or activities, such as a research study. In that case, any payment is a byproduct of the service provided. Thus, the payment by a research sponsor to a covered entity to conduct a research study is not considered a sale of PHI even if the research results that may include PHI are disclosed to the sponsor in the course of the study. Furthermore, receipt of a grant or funding from a government agency to conduct a program is not a sale of PHI even if, as a condition of receiving funding, the covered entity is required to report PHI to the agency for program oversight or other purposes.

Effect on Health Information Exchanges. HHS also clarified that exchange of PHI through a health information exchange (HIE) that is paid for through fees assessed on HIE participants is not a sale of PHI because the remuneration is for the services provided by the HIE and not for the data itself. In contrast, a sale of PHI occurs when the covered entity primarily is being compensated to supply data it maintains in its role as a covered entity (or business associate). Thus, such disclosures require an authorization unless they meet an exception.

Broad Definition of Remuneration. "Remuneration" for purposes of the sale provisions is not limited to financial payment as it is in the marketing provisions. Rather, it includes in-kind benefits unless another exception is met.

C. Research

Compound Authorizations. The Final Rule allows a covered entity to combine conditioned and unconditioned authorizations for research, provided the authorization *clearly differentiates* between the conditioned and unconditioned research components and allows the individual the option to opt in to the unconditioned research activities. HHS clarifies that it intends this provision to allow for the use of compound authorizations for any type of research activities, except to the extent the research includes use or disclosure of psychotherapy notes.

- **Examples Provided.** The Final Rule gives covered entities, institutions and institutional review boards flexibility to determine the best approach for clearly differentiating the conditioned and unconditioned research activities, and gives several examples of permissible approaches for distinguishing between conditioned and unconditioned research activities.

Authorizing Future Research Use or Disclosure. In a significant change, HHS modified its prior interpretation that research authorizations must be study specific. Under the revised interpretation, HHS permits an authorization for future research, to the extent the authorization adequately describes such purposes, such that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for such future research. HHS commentary indicates that this could include specific statements with respect to sensitive research to the extent such research is contemplated (subject to applicable state law). HHS also makes a number of other clarifications relevant to research authorizations in the commentary. An authorization must contain all other required elements.

D. Decedents

Privacy Rule Protections Expire 50 Years After Death. The HIPAA Privacy Rule was amended to provide that covered entities need only comply with the requirements of the HIPAA Privacy Rule with regard to PHI of a deceased individual for a period of 50 years following the date of death. Other laws (such as state sensitive information laws) may continue to protect such information beyond that point.

More Flexibility Re: Disclosures to Decedent's Family Members and Others Involved in Care. The Final Rule expressly permits covered entities to disclose a 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. Depending on the circumstances, this could include disclosures to spouses, parents, children, domestic partners, other relatives or friends of a decedent. Such disclosures must be limited to the PHI relevant to the particular family member's or other person's involvement in the individual's health care or payment for health care.

E. Disclosure of School Immunizations to Schools

Recognizing that schools play an important role in preventing the spread of communicable diseases among students, many states have "school entry laws" that prohibit a child from attending school unless the school has proof that the child has been appropriately immunized. The Final Rule recognizes that the HIPAA Privacy Rule as currently written may be hindering schools' achievements in such a role. To provide added flexibility, the Final Rule permits a covered entity to disclose proof of immunization to a school where (i) state or other law requires the school to have such information prior to admitting the student and (ii) the covered entity obtains agreement, which may be *oral or written*, from a parent or guardian or other person acting *in loco parentis* for the individual, or from the individual if the individual is an adult or an emancipated minor. Covered entities must document the agreement obtained. For example, if a parent requests over the phone that his child's immunization records be disclosed to the school, a notation in the child's medical record or elsewhere of this phone call would suffice for documentation of the agreement.

F. Fundraising

The Final Rule brings additional clarification and flexibility to the use and disclosure of PHI in a covered entity's fundraising activities. Highlights include:

Expanded PHI Available for Fundraising. The Final Rule clarifies and expands the scope of PHI a covered entity may use or disclose for fundraising. Currently, only "demographic information relating to an individual," health insurance status and dates of health care provided may be used. The Final Rule clarifies that "demographic information relating to an individual" includes name, addresses, other contact information, age, gender and dates of birth. It continues to allow use of health insurance status and dates of health care provided, but also now permits covered entities to use and disclose general department of service information (e.g., cardiology, oncology, etc.), treating physician information and outcome information (e.g., information regarding the death of the patient or any sub-optimal result of treatment or services) for fundraising purposes. As with any use or disclosure under the HIPAA Privacy Rule, a covered entity must use and disclose only the minimum amount of PHI necessary.

Flexibility on Fundraising Opt-Outs. Under the Final Rule, covered entities are required to include an opt-out mechanism with all fundraising communications (which includes any communication, written or oral, where there is an ask for a gift). However, the Final Rule allows flexibility as to the mechanism (such as toll-free number, email address or pre-paid, pre-printed postcard). It also allows covered entities to decide whether the opt-out applies to all future fundraising campaigns or to a specific campaign. Whatever opt-out process is selected, it cannot cause the individual undue burden or more than a nominal cost.

Need to Track Opt-Outs; Need for Affirmative Opt-In. Once an individual has opted out of fundraising communications, the covered entity must timely track and flag these individuals, and is prohibited from sending further fundraising communications to the individual unless the individual *affirmatively* opts back in.

G. Notices of Privacy Practices

A number of provisions under the Final Rule impact a covered entity's NPP. As a result, covered entities will need to evaluate their NPP, modify as necessary and redistribute consistent with the provisions of the Final Rule. Key areas of impact and redistribution requirements are noted below.

- **Certain Uses and Disclosures Requiring Authorization.** NPPs must now include a statement that most uses and disclosures of psychotherapy notes, uses and disclosures of PHI for marketing purposes and disclosures that constitute a sale of PHI require authorization. Furthermore, the NPP must reflect that any other uses and disclosures not specifically described in the notice will be made only with the individual's authorization.
- **Subsidized Treatment Communications.** Because the Final Rule treats all subsidized treatment communications as marketing communications, HHS did not adopt the proposal to require a statement in the NPP about such communications and the ability of an individual to opt out.

- **Fundraising.** NPPs must not only inform the individual if the covered entity intends to contact the individual to raise funds but also that the individual has the right to opt out of receiving such fundraising communications (in compliance with the fundraising requirements discussed above). Covered entities are not required (but may) include information about the opt-out mechanism in the NPP.
- **Right to Restrict Certain Disclosures to Health Plans.** *Health care providers* (but not other covered entities) are required to inform individuals in the NPP of their 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.
- **Breach Notice.** NPPs must include a basic statement as to an individual's right to be notified of a breach of unsecured PHI. HHS emphasizes that the statement need not be detailed or complex.
- **GINA.** Covered entity health plans that use or disclose PHI for underwriting purposes will need to revise their NPPs to state that such health plan is prohibited from using or disclosing genetic information for underwriting purposes, as discussed below.

H. Redistribution of Revised Notices of Privacy Practices

Health Plans. Under the Final Rule:

- A health plan that currently posts its NPP on its website must (i) prominently post the material changes to its NPP or its revised NPP on its website by September 23, 2013, and (ii) provide the revised NPP (or information about the material changes to the NPP and how to obtain a copy of the revised NPP) in the *next annual mailing* to individuals covered by the health plan.
- A health plan that does not maintain a customer service website is required to provide the revised NPP (or information about the material changes to the NPP and how to obtain a copy of the revised NPP) to individuals covered by the health plan within 60 days of the material revisions to the NPP.
- HHS reminds health plans that they must provide notices in a way that is accessible to all beneficiaries, including those with disabilities.

Health Care Providers. A health care provider with a direct treatment relationship with an individual must (i) make the NPP available upon request on or after the effective date of the revision, (ii) have the NPP available at the delivery site, and (iii) post the NPP (or summary with the full NPP "immediately available") in a clear and prominent position. HHS notes that providers are only required to give copies of the NPP to, and obtain a good faith acknowledgment of receipt from, new patients.

I. Right to Request a Restriction of Disclosures

In General. Under the Final Rule, a covered entity is required to permit individuals to restrict the disclosure of PHI about the individual to a health plan if: (A) the disclosure is for the purposes of carrying out payment or health care operations and is not otherwise required by law; and (B) the PHI pertains solely to a health care item or service for which the individual, or person on behalf of the individual other than the health plan, has paid the covered entity in full.

Operational Questions. HHS commentary goes into great detail on operational questions, including the following:

- **Segregating Versus Flagging Restricted Records.** These provisions do not require that covered health care providers create separate medical records or otherwise segregate PHI subject to a restricted health care item or service. Covered health care providers, however, will need to employ some method to flag or make a notation in the record with respect to the PHI that has been restricted to ensure that such information is not inadvertently sent to or made accessible to the health plan for payment or health care operations purposes, such as audits by the health plan.
- **Bundled Items/Services.** Where a provider is not able to unbundle a group of bundled items or services, the provider should inform the individual and give the individual the opportunity to restrict and pay out of pocket for the entire bundle.
- **Downstream Providers.** Health care providers (for example, a primary physician) are not required to alert downstream providers (for example, a specialist) of the fact an individual has requested a restriction to a health plan. Providers are encouraged to counsel and assist patients as feasible in alerting downstream providers of the individual's desire.

- **Other Guidance.** HHS also offers guidance for providers operating within an HMO context, disclosures in coordination-of-benefits contexts, situations where payment is dishonored, and situations involving follow-up care, among others.

J. Access of Individuals to Protected Health Information

The Final Rule amends a patient's right of access 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.

Flexibility in Business Associate's Role. HHS clarifies that the business associate's role in fulfilling access rights of the individual depends on the terms of the business associate agreement. There is no separate obligation for business associates to provide individuals with direct access to their health records, unless the business associate agreement so provides.

Requirements for Transmission to Third Parties Designated by the Individual. The Final Rule provides that, if requested by an individual, a covered entity must transmit an electronic copy of PHI directly to another person designated by the individual. In contrast to other requests under § 164.524, when an individual directs the covered entity to send the copy of PHI to another designated person, the request *must* be made *in writing, signed by the individual (including valid electronic signature), and clearly identify the designated person and where to send the copy* of the PHI. Also, HHS clarifies that if the request comes from the individual, it is not subject to the authorization provisions. Covered entities will want to make sure their access request procedures and forms reflect these requirements for transmission to third parties.

Clarification of Fees. HHS also provides a number of comments and clarifications regarding the charging of reasonable, cost-based fees for copies of PHI.

Timeliness. A covered entity must now provide an individual with access to off-site records within 30 days of the individual's request when possible, with a 30-day extension available (for a total of 60 days, in contrast to the current law that permits up to 90 days to provide the individual with access to such records).

IV. Modifications to the HIPAA Privacy Rule Under GINA

Citing an individual's strong interest in the way his or her genetic information is used for underwriting purposes, the Final Rule generally prohibits health plans that are covered entities under HIPAA from using or disclosing PHI that is genetic information for underwriting purposes. The Final Rule extends such prohibition to covered entities that are not expressly covered by GINA, except with regard to issuers of long-term care policies.

In issuing the Final Rule, HHS notes that while issuers of long-term care policies are exempt from the Final Rule's prohibition on using or disclosing genetic information for underwriting purposes at this time, it is looking further into how genetic information is used by such issuers and may issue additional guidance in the future.

The Final Rule makes clear that all covered entity health plans, including long-term care plans, continue to be bound by the HIPAA Privacy Rule as it relates to genetic information.

Covered entity health plans that are subject to the Final Rule's underwriting prohibition for genetic information will need to revise their NPPs accordingly.

V. Enforcement

To implement the HITECH Act, HHS issued an interim final enforcement rule establishing four categories of violations, with increasing penalty amounts reflecting increasing levels of culpability, and a maximum penalty amount of $1.5 million annually for all violations of an identical provision. It is important to note that one covered entity or business associate may be subject to multiple violations of multiple requirements, resulting in a total penalty above $1.5 million. In general, the categories are:

- "Did not know"—not less than $100 nor more than $50,000 for each violation.
- Due to reasonable cause and not willful neglect—not less than $1,000 nor more than $50,000 for each violation.
- Due to willful neglect and timely corrected (i.e., within the 30-day period beginning on the date that an entity first acquires actual or constructive knowledge of the violation)—not less than $10,000 nor more than $50,000 for each violation.
- Due to willful neglect *and* not timely corrected—not less than $50,000 for each violation.

The above penalties apply to both covered entities and business associates (including subcontractors). The Final Rule retains this penalty structure. Also, the Final Rule confirms and/or clarifies:

- The Secretary is required to investigate any complaint where "a preliminary review of the facts" indicates a possible violation due to willful neglect.
- The Secretary is required to conduct a compliance review when a preliminary review indicates a *possible* violation due to willful neglect (typically, this involves situations brought to the Department's attention other than through a complaint). The Secretary will continue to have discretion to conduct such a compliance review in circumstances not indicating willful neglect.
- The Secretary "may" (rather than must) attempt to resolve investigations or compliance reviews indicating non-compliance by informal means. This means the Secretary may move directly to a civil money penalty without exhausting informal resolution efforts. The Department will continue to have the ability to seek resolution of complaints and compliance reviews that do not indicate willful neglect violations by informal means.

Factors Considered in Determining the Amount of a Civil Money Penalty. The Secretary must consider the following factors in determining the amount of any civil money penalty:

- The nature and extent of the violation (consideration may include the number of individuals affected);
- The nature and extent of the harm resulting from the violation (consideration may include whether the violation caused physical, financial and/or reputational harm);
- The history of prior compliance with the administrative simplification provision, including violations by the covered entity or business associate (consideration may include whether the current violation is the same or similar to previous indications of non-compliance);
- The financial condition of the covered entity or business associate (consideration may include whether the covered entity or business associate had financial difficulties that affected its ability to comply); and
- Such other matters as justice may require.

The Final Rule does not modify the Secretary's discretion in how to apply the above-listed factors (i.e., as either mitigating or aggravating).

Now that the Final Rule has provided long-awaited definitive guidance to the industry on key HITECH Act changes, covered entities and business associates can expect to see enhanced enforcement.

****

For further information, please contact any member of Katten's Health Information Privacy and Security Group, or your regular Katten attorney.