Connecting Healthcare with Legal Excellence℠

Health Law Diagnosis

The HITECH "OMNIBUS RULE"

After waiting over two years from the publication of the Notice of Proposed Rulemaking to implement provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH NPRM), HHS finally released the final rule to implement the provisions of HITECH and amendments to HIPAA. Released on Thursday, January 17, 2013, the Final Rule totaled 563 pages pre-publication and implemented the majority of the proposed provisions from the HITECH NPRM. It was officially published in the Federal Register on January 25, 2013, and is set to become effective on March 26, 2013. Covered entities and business associates will be responsible for complying with the Final Rule no later than September 23, 2013, subject to certain transition provisions.

Brief Summary of the Final Rule

The Final Rule addressed broadly amendments to the HIPAA Privacy and Security Rules, as well as implementation of the new HITECH Breach notification requirements and enforcement provisions. Business associates and their subcontractors were dealt with extensively, with HHS clarifying the extent to which business associates and their subcontractors are directly liable for provisions of the Security Rule as well as Privacy Rule. HHS adopted provisions for how civil monetary penalties (CMPs) will be implemented in circumstances involving "willful neglect" as well as clarifying liability of covered entities for their "agents", including where a business associate may be considered an agent for purposes of Federal common law agency.

The Final Rule also adopted almost wholly the provisions proposed by the HITECH NPRM governing marketing, sale of PHI and fundraising. Authorizations will be required for communications that market a health-related product or service, with the proposed exceptions for treatment-related communications or appointment reminders where remuneration not retained. For the "sale" of PHI, HHS clarified what "sale" would include that would trigger an authorization requirement, and for fundraising, HHS retained the requirement that individuals be provided with the opportunity to "opt out" of fundraising communications. HHS also increased the amount of PHI which may be used for purposes of fundraising by covered entities and their business associates.

The Final Rule did not include final provisions for accountings of disclosures. In May of 2011, OCR issued a Notice of Proposed Rulemaking modifying the HIPAA Accounting of Disclosures requirement (AOD NPRM) as a result of HITECH amendments. The AOD NPRM would improve patient access to information about the individuals and entities that accessed their electronic health records, requiring provision of a separate access report to individuals that would detail all electronic accesses made to PHI maintained by a Covered Entity in its electronic designated record set. The AOD NPRM would also limit the types of disclosures that Covered Entities would have to account for.

However, the Final Rule did address access to electronic copies of health information afforded to individuals by HITECH, requiring that electronic copies be provided where an electronic designated record set was maintained, rather than an electronic health record. In addition, the Final Rule clarified the right afforded to individuals by HITECH to request restrictions on their health information where they pay out of pocket for health care items and services disclosed solely to a health care plan for purposes of payment or health care operations, discussing circumstances where services are bundled, downstream providers, or subsequent treatment which may require disclosure of previously restricted information to a health plan.

The Final Rule also modified previous HIPAA prohibitions on compound authorizations and research, permitting now conditional authorizations and unconditional authorizations to be combined in the research context, subject to certain requirements, as well as authorizations for future research permitted. The proposed revisions governing how decedent PHI is handled were also adopted, with the information of decedents who have been deceased for fifty or more years no longer being treated as PHI. The Final Rule also implemented several amendments to GINA, incorporating genetic information specifically as PHI, and restricting the majority of health plans from using genetic information for underwriting purposes.

Last, but not least, the Final Rule modified the "risk of harm" threshold adopted by the HITECH Interim Breach Notification Rule (2009). Although it remains in effect until the effective date of the Final Rule, impermissible uses and disclosures are now *presumed to be a Breach* ***unless*** it can be demonstrated a "low probability" exists that the PHI has been compromised or that an exception otherwise applies. In order to determine whether there is a low probability that PHI has been compromised, a "risk assessment" must be conducted. Covered entities are ultimately responsible for providing any required Breach notifications.

Enforcement

The Final Rule made changes to the HIPAA Enforcement Rule (2006) and HITECH Interim Final Enforcement Rule (2009) in order to implement HITECH's civil monetary penalties (CMPs) and new tiers of penalties, investigations involving potential willful neglect, and affirmative defenses. The Secretary is now required to investigate all complaints involving or possibly involving "willful neglect", which are subject to the imposition of CMPs, as well as permit the Secretary to resolve such complaints by informal action. The Secretary is required to also conduct a "compliance review" under such circumstances to determine the entity's compliance with applicable administrative simplification provisions. Covered entities and business

associates are required to disclose PHI and other information to the Secretary in connection with any investigations or compliance reviews.

Business associates, as well as covered entities, are directly liable for CMPs, where such may be applicable. The first category of violations and the lowest penalty tier established by HITECH cover circumstances under which a covered entity or business associate did not know, nor by exercising reasonable diligence would have known, of a violation. The second category involves violations due to "reasonable cause", which may avoid the imposition of a CMP, and the third and fourth categories apply to "willful neglect", corrected within 30 days (a significantly less penalty than where left uncorrected) or uncorrected, which are the highest penalty tiers.

The Final Rule modifies the definition of "reasonable cause" to clarify the state of mind, or *mens rea*, required. While no *mens rea* is required for violations under the first category, and *mens rea* is *presumed* for violations of the third and fourth categories, the previous definition of "reasonable cause" did not address the required *mens rea*. The new definition now includes violations due to circumstances making it unreasonable to comply with the provision which was violated, despite exercising ordinary business acre and produce, or where otherwise the covered entity or business associate had knowledge of a violation but lacked the "conscious intent" or "reckless indifference" associated with the willful neglect categories.

The Final Rule removed the exception for covered entity liability that had existed for the acts of an agent where such agent was a business associate, a HIPAA BAA had been entered into, the covered entity did not know of a pattern or practice of the business associate in violation of the contract, and the covered entity did not fail to act as required by HIPAA with respect to such. The Final Rule makes it clear that a covered entity, as well as a business associate, will be liable for the acts of its agents and subject to CMPs in accordance with Federal common law agency principles. Therefore, where a covered entity or business associate delegates out an obligation under HIPAA, that entity will remain responsible for the failure of an agent to perform such obligation on its behalf.

The Final Rule retains the penalty structure and maximum penalty amounts set forth in the HITECH Interim Final Enforcement Rule. It emphasizes, however, that HHS will not impose the maximum penalty amount in all cases, but rather, determine the penalty to be applied on a case-by-case basis, taking into account the nature and extent of the violation and resulting harm, including reputational. Other factors which will be taken into account include the financial condition and size of the covered entity or business associate. The Secretary remains able to waive, compromise on or settle any issue or concern involving a CMP.

Finally, the Final Rule retains the changes made by the HITECH Interim Final Enforcement Rule which removed the affirmative defense to imposition of penalties where the covered entity did not know and by exercising reasonable diligence would not have known (now the lowest tier of penalties) and prohibiting penalties where a violation, other than one due to willful neglect, was corrected within thirty days. In addition, the affirmative defense applicable of "criminally punishable" remains applicable where a covered entity or business associate can demonstrate that a criminal penalty has been imposed.

Business Associates

A covered entity is and has been required by HIPAA to enter into a HIPAA Business Associate Agreement (HIPAA BAA) with any entity that would create, receive or transmit PHI for or on their behalf in connection with certain health care operations purposes. However, before the implementation of the HITECH Act, business associates of covered entities were not directly liable for improper uses or disclosures of protected health information (PHI) in the performance of services or functions. HITECH resolved this, making provisions of the Privacy and Security Rules *directly applicable* to business associates, with the NPRM proposing modifications to the definition of a "business associate", including adding Patient Safety Organizations and patient safety activities as well as subcontractors, certain health information exchange organization (HIOs) and personal health record (PHR) activities.

The HITECH Final Rule makes business associates directly liable for provisions of the Security Rule. In addition, subcontractors of a business associate that create, receive, maintain or transmit PHI on behalf of such business associate are *likewise* ***HIPAA business associates***. Therefore, these downstream subcontractors will be subject to the same requirements that the first business associate is subject to. Each business associate now also is required to have a HIPAA compliant BAA in place with its subcontractors, its subcontractor with its own subcontractors, and so forth down the chain of subcontractors no matter how long.

The HITECH Final Rule modifies the definition of "business associate" to mean that a business associate is any person who "creates, receives, maintains, or transmits" PHI on behalf of a covered entity, in order to clarify that *any entity that maintains PHI*, such as a data storage organization, is a business associate *even if it does not access or view the PHI.* PHRs vendors will also be considered business associates where they provide PHRs for or on behalf of a covered entity, rather than simply establishing a connection for the covered entity to send PHI to the individual's PHR. Rather than acting simply as a "conduit", the PHR vendor is maintaining PHI on behalf of the covered entity for the benefit of the individual.

For HIOs and other entities, they will be considered business associates where they (1) provide data transmission services with respect to PHI and (2) require routine access to the PHI. The Preamble to the HITECH Final Rule clarifies "access on a routine basis" to mean circumstances where an entity requires access to PHI in order to perform services and functions on behalf of a covered entity, such as management of an exchange network through use of record locator and other services on behalf of its participants. However, HHS recognizes that it will depend upon the circumstances and states its intention of issuing future guidance in this area.

The HITECH Final Rule also provides some clarification as to when a business associate will be an "agent" of a covered entity. Although generally determinations of whether a business associate will be acting as an agent of a covered entity are fact specific and will depend upon the totality of the circumstances of the relationship between the parties, the Final Rule makes it clear that federal common law agency principles will be applied, regardless of whether the parties consider or state themselves to be independent contractors. If the covered entity has

the right to control or direct any given service or function provided or performed by the business associate, then an agency relationship will likely be created (i.e., where a covered entity directs how a business associate will make available access to PHI by an individual).

Liability for a business associate's actions, however, will only extend to the scope of the agency. For example, if a business associate fails to limit PHI disclosed to the minimum necessary while performing services it was engaged by a covered entity to perform (as an agent), then the business associate is likely acting within the scope of agency. However, a business associate's conduct is outside the scope of agency where it acts for its own benefit or for that of a third party.

Business associates are also subject to the HITECH marketing requirements, to be discussed in a future blog post. And finally, the HITECH Final Rule applies certain other provisions of the Privacy Rule directly to business associates. Business associates will have direct liability for impermissible uses or disclosures in violation of the HIPAA BAA or the Privacy Rule, as well as: (i) failure to disclose PHI where required by the Secretary; (ii) failure to disclose PHI for purposes of affording an individual's access rights; (iii) failure to limit PHI used/disclosed to the minimum necessary; (iv) failure to obtain a HIPAA compliant BAA with subcontractors; (v) failure to provide breach notification; and (vi) failure to provide an accounting of disclosures (subject of a separate future rulemaking).

Covered entities and business associates are permitted under the Final Rule transition provisions to continue operating under existing HIPAA BAAs for up to one year beyond the compliance date of the Final Rule, or initial renewal/modification, whichever earlier. The minimum requirements of a HIPAA BAA were slightly modified by the Final Rule, and now:

1. Must include the requirement that a business associate report any Breach of which it becomes aware to the covered entity, in addition to security incidents;

2. Must include the requirement that a business associate, to the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, comply with the requirements that apply to the covered entity in the performance of such obligation; and

3. Need not include the requirement that the covered entity report a business associate to the Secretary for patterns or practices which constitute a material breach or violation of the HIPAA BAA.

Breaches and Harm Standard

The HITECH Interim Breach Rule defined a Breach to mean generally "the acquisition, access, use, or disclosure of protected health information in a manner not permitted [by the Privacy Rule] which compromises the security or privacy of the protected health information." It further elaborated that "compromises the security or privacy of the PHI" meant *poses a significant risk of financial, reputational, or other harm to the individual.* HHS explained that it originally included this "harm" standard in order to align the rule with many State breach

notification laws as well as existing obligations on Federal agencies that have a similar "risk of harm" standard for triggering breach notification.

The HITECH Final Rule removes the '*significant risk of harm*' test, and **replaces it with a presumption** that *any* impermissible use or disclosure of PHI is *presumed to be a* ***breach*** *unless* the CE or BA, as the case may be, demonstrates that there is a ***low probability*** that the PHI has been compromised. A covered entity or business associate essentially has the ***burden of proof*** to demonstrate that there is a low probability that the PHI is compromised. The CE and BA must also maintain written documentation sufficient to demonstrate why it concluded that there is a low probability that the PHI was compromised and did not issue breach notification.

The HITECH Final Rule *requires* that the covered entity or business associate conduct a *Risk Assessment* in order to determine whether a low probability exists that the PHI has been compromised. At a minimum, the following **four factors** are required as part of the Risk Assessment:

1. Nature & Extent of PHI. For this factor, HHS suggests that covered entities and business associates consider the *type* of PHI involved, such as if the PHI was of a more "sensitive" nature. An example given is if credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud are involved, then this would ***cut against*** finding that there is "low probability" that the PHI was compromised. With respect to clinical information, HHS points out that CEs and BAs might consider things like the *nature of the services*, as well as the *amount* of information and *details* involved. It is worth noting that in a footnote, HHS specifically calls out that "sensitive" information is not just information that includes reference to STDs, mental health or substance abuse.

2. Unauthorized Person. To evaluate the second factor, HHS suggests that covered entities and business associates consider who the unauthorized recipient is or might be. For example, if the recipient person is someone at another covered entity or business associate, then this may support a finding that there is a lower probability that the PHI has been compromised since such entities are obligated to protect the privacy and security of PHI in a similar manner as the covered entity or business associate from where the breached PHI originated. Another example given is if PHI 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. Acquired or Viewed. The third factor requires covered entities and business associates to investigate and determine if the PHI was *actually* acquired or viewed or, alternatively, if only the *opportunity existed* for the information to be acquired or viewed. One example given here, a common scenario that arises for many covered entities and business associates, is where a covered entity mails information to the wrong individual who opens the envelope and calls the covered entity to say that he/she received the information in error. HHS points out that in such a case, the

unauthorized recipient viewed and acquired the information because he/she opened and read the information and so this cuts against a finding that there is low probability that the PHI was compromised. To contrast, HHS offers an example of how to analyze this factor in the context of lost laptops. Specifically, HHS explains that if a laptop computer is stolen and later recovered and a forensic analysis shows that the otherwise unencrypted PHI on the laptop was never accessed, viewed, acquired, transferred, or otherwise compromised, the covered entity or business associate could determine that the information was *not* *actually* acquired by an unauthorized individual even though the opportunity existed. However, here HHS is also quick to point out that if a laptop is lost or stolen, HHS would **not consider it *reasonable* to delay breach notification** based on the hope that the computer will be recovered and that forensics might show that the PHI was never accessed.

4. Mitigation. The final factor to analyze is mitigation. A covered entity or business associate must attempt to mitigate the risks to PHI following any impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the PHI will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed. When determining the probability that the PHI has been compromised, covered entities and business associates should consider the extent of what steps needed to be taken to mitigate, and how effective the mitigation was. HHS offered an example that covered entities and business associates 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 PHI it received in error, while such assurances from *certain* third parties may not be sufficient.

In the end, covered entities and business associates (and now, sub-vendors of business associates as well) just want to know what they should do in response to breaches. The general answer is that the **scales have tipped towards notifying affected individuals in *most* cases where PHI gets into the hands of someone who was not intended to have it.**

Access Rights & Restrictions

Under HITECH, individuals were granted the right to request and have access to electronic copies of their health information where such was maintained in an electronic health record (EHR). The HITECH Final Rule extends this to any PHI maintained **electronically** in a **designated record set**. Where "readily producible", an individual may request and receive an electronic copy of such PHI in any form and format, such as a PDF or Word document. Where the copy would not be readily producible in the form and format requested by the individual, the covered entity must work with the individual to agree on an alternate electronic form and format. A covered entity is also required to provide or transmit the copy of PHI to a third person where clearly designated by the individual in writing.

For hybrid records, both hard copy and electronic copies may be provided to the individual. Covered entities are permitted to charge reasonable cost-based fees for providing the copies of PHI (both for paper and electronic form), including the cost of providing portable media or postage for mailing the information. Covered entities may not charge individuals any

costs for technology, maintenance, storage, or retrieval fees for providing electronic copies. Covered entities no longer may have an additional thirty days where PHI is maintained off-site, and therefore must provide copies within thirty days, subject to one additional extension of thirty days.

In addition, HITECH granted individuals the right to request restrictions on disclosures to **heath plans** where the purpose of the disclosure is solely for **payment or health care operations purposes** and not otherwise required by law, and the individual, or his or her representative, has paid **out of pocket and in full** for the health care item or service. Covered entities and their business associates are required to comply with and implement such restrictions. In practicality, the out-of-pocket restriction requirement will only apply to *health care providers*.

The HITECH Final Rule retained this requirement despite public concerns about implementing restrictions. HHS notes that covered entities should be familiar with restrictions on disclosures of information given the minimum necessary standards, and should therefore have mechanisms in place to limit PHI disclosed to a health plan. HHS specifically also notes that covered entities are not required to segregate PHI or create separate medical records in order to implement restrictions, however, they must be able to "flag" or otherwise note a restriction has been implemented to ensure the information is not inadvertently sent to a health plan. Where a restriction has been implemented but a disclosure would be "required by law" (i.e., Medicare plans), the covered entity is permitted to disclose the information.

HHS also addressed "bundled" services and downstream disclosures where a restriction has been requested by the individual. A health care provider is required to "un-bundle" a health care item or service which is provided with other health care items/services in a single patient encounter to the extent it has been able to do so in order to implement a requested restriction. To the extent the health care provider is unable to do so, the health care provider must notify the patient of its inability to do so, the impact of doing so (i.e., the health plan can still determine from the context what the restricted information is), and give the individual the option of extending the restriction to all of the health care items/services.

HHS acknowledged it would be unworkable to require a health care provider notify other providers "downstream" of a restriction implemented for a disclosure to a health plan. As such, it encourages providers to discuss with their patients the need to notify each provider in order to prevent the information from being disclosed to the health plan, as well as assisting patients, as feasible, to alert other providers downstream of the requested restriction. For example, HHS notes that a health care provider prescribing medication to an individual who wishes to restrict disclosure of that medication to his or her health plan could provide a paper prescription, rather than transmitting it electronically to the pharmacy, in order to allow the patient to pay at the pharmacy before it is transmitted to the health plan for payment.

Marketing & "Sale" of PHI

The HIPAA Privacy Rule required covered entities to obtain authorizations from individual prior to using or disclosing PHI for marketing purposes. However, certain forms of

treatment and health care operations communications were excepted from the definition of "marketing" and therefore, did not require authorization from the individual. HITECH amended the marketing provisions, however, limiting the types of communications which may be considered "health care operations" except from the marketing requirements. In cases where the covered entity receives direct or indirect payment in exchange for making such communications, a written authorization is required from the individual before the communication can be made. HITECH included an exception for communications which describe only a drug or biologic currently being described to the individual provided any payment received was reasonable in amount.

The HITECH Final Rule adopts the term "financial remuneration" in order to clarify that payment, as defined by the Privacy Rule, was permitted for treatment of the individual. Financial remuneration means direct or indirect payment *from or on behalf of a third party whose product is being described in the communication.* In recognition of the confusion in distinguishing treatment communications between providers and their patients from health care communications, the HITECH Final Rule requires authorization for *all treatment and health care operations communications where financial remuneration would be received in exchange for making the communication.* The marketing restriction applies also to circumstances where a business associate (including a subcontractor) would receive financial remuneration from a third party in exchange for making a communication about a product or service.

The Privacy Rule face-to-face and nominal value exceptions for marketing communications are retained by the HITECH Final Rule. In addition, HHS clarified that, with regard to the HITECH exception for communications which describe only a drug or biologic, payment amounts must be "reasonably related" to the covered entity's cost of making the communication. Permissible costs include labor, supplies and postage to make the communications. Where "profit" or payment for other costs would be received, the financial remuneration, HHS states, would run "afoul" of the "reasonable in amount" requirement of HITECH.

HITECH also placed restrictions on the "sale of PHI", prohibiting the exchange of PHI for remuneration without the individual's authorization. However, HITECH excepted (1) public health activities, (2) certain research activities, provided the only remuneration received is reasonable and cost-based to cover the cost to prepare/transmit the PHI, (3) treatment of the individual, (4) sale, transfer or merger of the covered entity, (5) business associate services, (6) provision of access to an individual and (7) other purposes authorized by the Secretary of HHS. The HITECH Final Rule added to these exceptions, permitting also those disclosures required by law, and those authorized by the Privacy Rule where only "reasonable cost-based fees" were received to cover the cost to prepare and transmit PHI.

According to the HITECH Final Rule, "sale of PHI" means a disclosure of PHI by a covered entity (or business associate) where the covered entity (or business associate) directly or indirectly received remuneration, financial or otherwise, from or on behalf of the recipient of the PHI *in exchange* for the PHI. HHS clarifies that "sale" is not limited to circumstances where a transfer of ownership occurs, and would include "access, license or lease agreements." However, fees for participating in an HIO would not be considered a "sale." Rather, the

remuneration received is in exchange for the services provided by the HIO.

HHS states that a sale of PHI only occurs when the covered entity (or business associate) is being *primarily compensated to supply data it maintains in its role as covered entity or business associate.* Authorizations obtained for the sale of PHI must state that the covered entity is receiving remuneration in exchange for the disclosure of PHI, and whether the recipient may further exchange the PHI for remuneration.

Fundraising

The HIPAA Privacy Rule originally permitted only limited information to be used by a covered entity, its business associate or foundation for fundraising purposes. Only demographic information (including health care status) and dates of health care provided to an individual could be used and disclosed for fundraising purposes without an authorization from the individual. Covered entities were also required to include in their Notice of Privacy Practices a description of whether the covered entity intended to conduct fundraising, as well as a description in any fundraising materials of how an individual may opt-out of receiving future fundraising communications.

The HITECH Final Rule implements the HITECH requirement that a "clear and conspicuous opportunity" to opt-out of future fundraising communications be provided to the individual, as well as that if the individual opts-out, it must be treated as a revocation of authorization under the Privacy Rule. In addition, the method for an individual to opt-out must not impose an undue burden or more than a nominal cost on the individual. HHS states that covered entities should consider using toll-free numbers, email addresses or similar opt-out mechanisms that are simple, quick and inexpensive. Requiring an individual to send a written letter opting out of fundraising communications would constitute an undue burden, although a pre-printed, pre-paid postcard would be permitted.

The HITECH Final Rule also permits covered entities to determine whether it will permit opt-outs for all future communications, or just specific to a particular fundraising campaign. Once implemented, however, the covered entity must not send further such fundraising communications. The covered entity's Notice of Privacy Practices must include a statement regarding fundraising activities and that the individual may opt-out of receiving such communications. Treatment or payment may not be conditioned on the individual's choice to opt-out of a fundraising communication.

Finally, the HITECH Final Rule expands the types of PHI which may be used and disclosed for fundraising purposes. In addition to demographic information, health care status (considered separate from demographic information by HHS) and dates of health care, the HITECH Final Rule permits use and disclosure of information relating to the department of service (i.e., oncology, cardiology), treating physician information, and outcome information (i.e., information regarding the death or sub-optimal result of treatment or services) for fundraising purposes. HHS notes these three were the most frequently identified categories of information needed for covered entities to target fundraising to appropriate individuals. The minimum necessary standard continues to apply to use and disclosure for these types of

information for fundraising purposes.

Research and Immunizations

In general, the HIPAA Privacy Rule prohibits conditioning treatment, payment and certain enrollment or eligibility for benefits on an individual signing an authorization for disclosure except in the research context where the provision of research-related treatment could be conditioned on an individual signing an authorization that permits PHI to be used or disclosed for research purposes. In addition, the Privacy Rule prohibits generally the use of compound authorizations, except in the case of research studies which authorization may authorize use or disclosure of PHI as well as other written permission for the same study. In addition, the Privacy Rule prohibited the use of a compound authorization where one purpose of the authorization could be conditioned, and the other purpose could not be conditioned. This resulted in the research community having to obtain separate authorizations for clinical trials and other activities and causing inconsistency with other federal research regulations and confusion among research participants.

The HITECH Final Rule modified the HIPAA authorization requirements for research permitting compound authorizations. A covered entity may combine conditioned and unconditioned authorizations for research, *provided* that the authorization clearly distinguishes between the conditioned and unconditioned components, and permits the individual to opt-out of the unconditioned activities. In addition, *future research purposes* may be authorized by the same research authorization, and "purpose" will no longer be interpreted by HHS to mean study specific. The Privacy Rule had previously been interpreted by HHS to disallow any authorization for research which was not study specific; that is, did not describe each purpose for which PHI would be used or disclosed for research.

The HITECH Final Rule also modified the permissible HIPAA public health disclosures. Public health disclosures are permitted by the Privacy Rule without the individual's authorization, for example, immunization records could be disclosed to a state immunization registry. However, under the Privacy Rule, a health care provider would need to obtain authorization prior to disclosing immunization records for a school for purposes of school entry where the school requested such. The HITECH Final Rule permits disclosures by health care providers to schools for immunization purposes, provided that (1) the individual is a student or prospective student of the school, (2) the PHI disclosed is limited to proof of immunization, (3) the school is required by State or other law to have proof of immunization prior to admitting the individual, and (4) the health care provider obtains and documents (i.e., notation in the medical record of the individual) agreement to the disclosure from either a parent, guardian or other person acting *in loco parentis*, if an unemancipated minor, or the individual him or herself, if an adult or emancipated minor.

Genetic Information and Decedents

The Genetic Information Nondiscrimination Act of 2008 (''GINA''), Public Law 110–233, 122 Stat. 881, prohibits discrimination based on an individual's genetic information in the health coverage and employment contexts. The Final HITECH Rule expressly includes "genetic

information" as protected health information subject to HIPAA, additionally prohibiting most health plans subject to the Privacy Rule from using and disclosing genetic information for **underwriting purposes**. Issuers of long-term care policies, however, are not subject to this prohibition. Genetic information generally includes (1) the individual's genetic tests; (2) the genetic tests of family members of such individual; and (3) the manifestation of a disease or disorder in family members of such individual. A health plan may, however, use and disclose genetic information for other purposes, such as determining medical necessity of services provided or benefits, or making payment for such services.

The HITECH Final Rule also makes the health information of individuals who have been deceased for fifty (50) or more years no longer PHI and therefore not subject to the protections of HIPAA at that point. HHS stated it believes this will reduce the burden on covered entities and those seeking information on such decedents from having to locate a personal representative of the decedent. In addition, the HITECH Final Rule permits covered entities to disclose PHI of a decedent to those family members, relatives or other caretakers involved in the care or payment for such care of the decedent prior to his or her death.

Notice of Privacy Practices

In order to appropriately reflect all of the HITECH changes, Notices of Privacy Practices will need to be updated by covered entities. In particular, the NPP will need to reflect an individual's right to have access to electronic copies of PHI, as well as the right to request restrictions on disclosures to health plans for health care operations and payment purposes where the individual paid in full out of picket. For covered entities that conduct fundraising activities, they will need to include a fundraising statement and that the individual has a right to "opt out" of receiving such communications. In addition, the HITECH Final Rule requires a short statement that the individual has a right to notification in the event of a breach.

The NPP must also include a statement regarding marketing and "sale of PHI" activities, and that an authorization will be required for such activities, as well as for disclosure of psychotherapy notes. For covered entities that are health plans and which intend on using or disclosing genetic information, a statement must also be included that genetic information may not be used or disclosed for underwriting purposes. An authorization cannot be obtained in order to use or disclose genetic information for underwriting purposes.

* * * *

For more information, please contact:

Helen Oscislawski, Esq.
Principal at Oscislawski LLC
tel: 609-385-0833, ext. 1
helen@oscislaw.com

OR

Krystyna Monticello, Esq.
Partner at Oscislawski LLC
tel: 609-385-0833, ext. 2
kmonticello@oscislaw.com

Attorneys at Oscislawski LLC is a health law firm with its main office located in Princeton, New Jersey but a nationwide reputation for experience with and understanding of federal and state privacy and security laws, as well as electronic health information exchange, health information technology, and managing health data breaches. Our attorneys also advise clients on wide-range of other legal issues. For more information about our firm visit www.oscislaw.com. ***For excellent compliance information, tools and solutions, please also visit our affiliated blog & resource website*** *www.legalhie.com.*