Law Offices of
Robert A. Polisky

10100 Santa Monica Blvd.
Suite 300
Los Angeles, CA 90067
rpolisky@rphealthlaw.com

Main: 310.405.0888
Toll Free: 888.959.3577
Fax: 310.405.0886
www.rphealthlaw.com

February 7, 2013

Health Law Alert

2013 HIPAA Final Omnibus Rule: Expanded Applicability and New Obligations

On January 17, 2013, the Office for Civil Rights of the U.S. Department of Health & Human Services ("OCR") released a much-anticipated 563-page pre-publication version of the final omnibus rule (the "Final Rule"), implementing changes to the Privacy, Security, Breach Notification, and Enforcement Rules under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), many of which are required by the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"). The Final Rule, which was published on January 25, 2013 in the *Federal Register*, also implements changes to the Genetic Information Nondiscrimination Act of 2008.

The scope of the Final Rule is extensive, and enhances OCR's ability to enforce HIPAA. In the press release announcing the Final Rule, OCR's Director proclaims that the Final Rule "marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented" and "strengthen[s] the ability of my office to vigorously enforce the HIPAA privacy and security protections…." Individuals and entities affected by the Final Rule must comply with most of its provisions by September 23, 2013.

This Health Law Alert summarizes key provisions of the Final Rule, discusses enforcement changes, and concludes with recommended action items needed for compliance.

KEY PROVISIONS

Business Associates and Their Subcontractors

Expanded Definition of "Business Associate"

The Final Rule expands the definition of a "business associate" to include any individual or entity that creates, receives, maintains, or transmits protected health information ("PHI") on behalf of a covered entity. By adding "maintains" to the definition of "business associate", a data storage company that maintains PHI on behalf of a covered entity will now be considered a business associate, even if it does not view the PHI. The Final Rule also specifically designates the following as business associates: (i) patient safety organizations; (ii) health information organizations, e-prescribing gateways, and others that provide data transmission services involving PHI to a covered entity and that require routine access to such PHI; and (iii) vendors that offer a personal health record to an individual on behalf of a covered entity.

Notably, the Final Rule includes subcontractors that create, receive, maintain, or transmit PHI on behalf of a business associate as business associates themselves.

OCR estimates that there are approximately one to two million business associates and an unknown number of subcontractors that are subject to the Final Rule.

Direct Liability

The Final Rule requires business associates to comply with the Security Rule's administrative, physical, and technical safeguards requirements, as well as with the Security Rule's policies and procedures and documentation requirements. These requirements apply to business associates in the same manner as they apply to covered entities, such that business associates can be held civilly and criminally liable for violations of these requirements. Similarly, the Final Rule applies certain Privacy Rule requirements to business associates and establishes direct liability of business associates for violations of these requirements; a business associate does not need to provide a notice of privacy practices ("NPP") or designate a privacy official, unless the covered entity designated such a responsibility in a business associate agreement.

Specifically, a business associate has direct civil and criminal liability exposure 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 either the covered entity, the individual, or the individual's designee (whichever is specified in the business associate agreement);
- Failure to disclose PHI to OCR where required by OCR to investigate or determine the business associate's compliance with HIPAA;
- Failure to provide an accounting of disclosures;
- Failing to enter into business associate agreements with subcontractors that create or receive PHI on the business associate's behalf; and
- Failure to comply with the requirements of the Security Rule.

A business associate also remains contractually liable for all other Privacy Rule obligations that are included in its business associate agreement with a covered entity.

Business Associate Agreements

The Final Rule clarifies that a covered entity is not required to enter into a business associate agreement with a business associate's subcontractor. Rather, the business associate that has engaged the subcontractor to perform a function or service involving the use or disclosure of PHI is required to enter into a business associate agreement with the subcontractor. Each business associate agreement in the business associate chain needs to be as or more restrictive than the agreement above it in the chain with respect to permissible uses and disclosures of PHI.

The Final Rule expands the requirements of a business associate agreement by obligating a business associate to: (i) comply, where applicable, with the Security Rule with regard to electronic PHI; (ii) report breaches of unsecured PHI to the covered entity; and (iii) ensure that any subcontractors that create or receive PHI on its behalf agree to the same restrictions and conditions that apply to the business associate with respect to such information.

Transition Period

The Final Rule delays compliance until September 22, 2014 for a covered entity or business associate to enter into a business associate agreement with a business associate or subcontractor if, prior to January 25, 2013, the covered entity or business associate had a business associate agreement with the business associate or subcontractor, as applicable, that complied with HIPAA prior to the Final Rule, unless the business associate agreement was modified or actively renewed between March 26, 2013 and September 23, 2013. In all other cases, covered entities and business associates will need to execute business associate agreements with their business associates and subcontractors no later than September 23, 2013.

Modification to Breach Notification Rule

Background

Under the HITECH Act, a covered entity is required to notify affected individuals and OCR following discovery of a breach of unsecured PHI; a covered entity also needs to notify the media of a breach involving more than 500 residents of a State or jurisdiction. A business associate, in turn, is required to notify a covered entity following discovery of a breach of unsecured PHI at or by the business associate.

On August 24, 2009, OCR issued an interim final rule implementing the HITECH Act's breach notification provisions ("Breach Notification Interim Rule"). In the Breach Notification Interim Rule, a "breach" is defined as the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule that "compromises the security or privacy" of the PHI, with certain exceptions. Moreover, under the Breach Notification Interim Rule, "compromises the security or privacy" of the PHI means that an impermissible use or disclosure of PHI poses a significant risk of financial, reputational, or other harm to the individual (the "harm standard").

Revised Definition of "Breach"

The Final Rule significantly revises the definition of "breach" to clarify that an impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised. By replacing the "harm standard" with this "low probability" standard, it is more likely under the Final Rule than under the Breach Notification Interim Rule that covered entities and business associates will determine that an impermissible use or disclosure of PHI "compromises the security or privacy" of the PHI, resulting in many required breach notifications that would not have been required previously.

Modification of Risk Assessment

Under the Final Rule, to determine whether there is a low probability that PHI has been compromised, covered entities and business associates need to conduct a risk assessment that considers at least the following factors:

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

If an evaluation of the above factors, taken together, fails to demonstrate that there is a low probability that PHI has been compromised, breach notification will be required.

Marketing

Currently, HIPAA does not require an individual's authorization for a marketing communication that uses or discloses the individual's PHI if the communication is for treatment or healthcare operations. The Final Rule limits this exception by requiring an individual's authorization if a covered entity receives financial remuneration from a third party to market its product or service. In such cases, the authorization must disclose that the covered entity received financial remuneration from a third party for making the marketing communication. For example, prior to the Final Rule, an imaging center would not need to obtain authorization to send marketing collateral to patients about new mammography equipment where the equipment's manufacturer paid for the collateral, but, under the Final Rule, the center would need to do so.

In addition, the Final Rule retains the exception to needing an authorization for drug or biologic refill reminders or otherwise to communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication. The Final Rule also retains exceptions to needing authorization for marketing communications that are face-to-face communications or consist of only promotional gifts of nominal value provided to an individual.

Sale of PHI

The Final Rule prohibits the sale of an individual's PHI without the individual's authorization, except:

- For public health purposes;
- For research purposes where the only remuneration received by the covered entity or business associate 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 for related due diligence;
- To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;
- To the individual, when requested;
- For disclosures required by law; and
- For any other purpose permitted by and in accordance with the applicable requirements of the Privacy Rule, where the only remuneration received by the covered entity or business associate 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.

The authorization must state that the disclosure will result in remuneration to the covered entity.

The Final Rule defines "sale of PHI" as a disclosure of PHI by a covered entity or business associate 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. Notably, the Final Rule does not limit a "sale" to only transactions where there is a transfer of ownership of PHI, and includes, as a "sale", disclosures in exchange for remuneration that are the result of access, license, or lease agreements.

Fundraising

Currently, HIPAA allows a covered entity to use, or disclose to a business associate or an institutionally related foundation, only the following types of PHI about an individual for the covered entity's fundraising from that individual, without the individual's authorization: (i) demographic information relating to the individual; and (ii) the date(s) of service provided to the individual. The Final Rule adds the following types of PHI that can be used for fundraising from an individual without the individual's authorization, enabling more targeted fundraising: (i) department of service information; (ii) treating physician information; (iii) outcome information; and (iv) health insurance status.

In each fundraising communication made to an individual, a covered entity must provide the individual with a clear and conspicuous opportunity to opt out of further solicitations; covered entities can determine the method an individual can use to opt out, as long as the method does not cause an individual to incur an undue burden or more than a nominal cost. After individuals opt out, a covered entity cannot send any fundraising communication to them. The Final Rule also specifies that a covered entity may not condition treatment or payment on an individual's choice whether or not to receive fundraising communications. The Final Rule permits a covered entity to provide an individual who has opted out with a method to opt back in to receive fundraising communications.

Notice of Privacy Practices

As background, the Privacy Rule requires that most covered entities have and distribute an NPP to individuals. The NPP needs to describe the uses and disclosures of PHI a covered entity is allowed to make, the covered entity's legal duties and privacy practices with respect to PHI, and the individual's rights concerning PHI.

To ensure that individuals are aware of the HITECH Act's changes that affect privacy protections and individual rights regarding PHI, the Final Rule requires covered entities to modify their NPPs by including statements that:

- Most uses and disclosures of psychotherapy notes (where appropriate), uses and disclosures of PHI for marketing purposes, and disclosures that constitute a sale of PHI require authorization;
- Other uses and disclosures not described in the NPP will be made only with authorization;
- If the covered entity intends to contact an individual to raise funds for the covered entity, PHI may be used and disclosed for fundraising communications, and an individual has a right to opt out of receiving such communications; the NPP does not need to include the opt out method;
- Individuals have a right to restrict certain disclosures of PHI to a health plan where the individual pays out of pocket in full for the healthcare item or service (only healthcare providers need to include this statement);
- Affected individuals have a right to be notified following a breach of unsecured PHI; OCR clarified that this simple statement suffices for purposes of addressing the breach notification rule in an NPP; and
- The covered entity is prohibited from using or disclosing PHI that is genetic information for underwriting purposes (only health plans need to include this statement).

Access of Individuals to Electronic PHI

The Final Rule amends the Privacy Rule by providing that, if an individual requests an electronic copy of PHI that is maintained electronically in one or more designated record sets (regardless of whether the designated record set is an electronic health record), a covered entity must provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format, or, if it is not, in a readable electronic form and format as agreed to by the covered entity and the individual. OCR states that a covered entity is not required to purchase new software or systems in order to accommodate an electronic copy request for a specific format that the covered entity cannot readily produce at the time of the request, so long as the covered entity is able to provide some form of electronic copy. OCR notes that some legacy or other systems may not be capable presently of providing any form of electronic copy and anticipates that some covered entities may need to invest in technology in order to be able to provide some form of electronic copy. If the individual does not accept any of the electronic formats that are readily producible by the covered entity, the covered entity must provide a hard copy as an option to fulfill the access request.

OCR clarifies that, if an individual requests that a copy of his or her PHI be sent by unencrypted email, a covered entity is permitted to send the email, so long as the covered entity has advised the individual of the security risk and the individual still wants to receive the unencrypted email.

The Final Rule allows a covered entity to charge a reasonable cost-based labor fee for copying electronic PHI, which can include time spent to create and copy the electronic file, such as compiling, extracting, scanning, and burning PHI to media, and distributing the media. The Final Rule also allows a covered entity to charge for the cost of supplies for creating the paper copy or electronic media (e.g., CD or USB flash drive), if an individual requests that the electronic copy be provided on portable media. Further, the Final Rule allows a covered entity to charge for the cost of postage, if the individual requests that the portable media be sent by mail or courier. Importantly, however, the Final Rule does not allow a covered entity to charge any retrieval fee related to an individual's request.

Designation of Third Party to Receive PHI

The Final Rule provides that, if requested by an individual, a covered entity must transmit a copy of the individual's PHI directly to another person designated by the individual, so long as the individual's request is in writing, signed by the individual, and clearly identifies the designated person and where to send the copy of PHI. This requirement applies to PHI in paper and electronic form.

Research

The Final Rule allows an authorization for the use or disclosure of PHI for a research study to be combined with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. The Final Rule requires that where a covered healthcare provider conditioned the provision of research-related treatment on one of the authorizations, any compound authorization must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

PHI of Decedents

Currently, the Privacy Rule requires covered entities to protect the privacy of a decedent's PHI indefinitely and generally in the same manner and to the same extent that is required for PHI of living individuals. The Final Rule limits the period of protection of a decedent's PHI to 50 years after his or her death; this limitation only sets the outer limit of HIPAA protection for this PHI and does not, by itself, require that PHI be retained for 50 years after death. Also, the Final Rule allows covered entities to disclose a decedent's PHI to family members, friends, 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 decedent that is known to the covered entity.

Student Immunization Records

The Final Rule permits covered entities to disclose to a school proof of immunization of a student or prospective student if: (i) the school is required by law to have proof of immunization; and (ii) the covered entity obtains and documents that the student (if an adult or emancipated minor), or the parent or guardian, agreed orally or in writing to the disclosure.

Right to Restrict Disclosure to a Health Plan

Under the Final Rule, healthcare providers, upon request from an individual, must agree to restrict disclosure of PHI about the individual to a health plan if: (i) the disclosure would be for the purpose of carrying out payment or healthcare operations, and is not otherwise required by law; and (ii) the PHI pertains solely to a healthcare item or service for which the individual, or person acting on the individual's behalf (other than the health plan), has paid the covered entity in full. To avoid payment issues, a healthcare provider may want to require payment in full at the time of the individual's request for a restriction.

ENFORCEMENT

Discretion

The Final Rule gives OCR discretion to use informal means to resolve HIPAA violations. However, OCR is permitted to impose a civil monetary penalty without exhausting informal resolution efforts, especially when the HIPAA violation is due to willful neglect. The Final Rule also allows OCR to coordinate with other law enforcement agencies, such as State Attorneys General and the Federal Trade Commission, with respect to pursuing remedies against HIPAA violators.

Tiered Penalty Amounts

Under the HITECH Act, there are four tiers of increasing penalty amounts that correspond to the levels of culpability associated with a HIPAA violation. The minimum fines range between $100 and $50,000 per violation, and are capped at $1.5 million for all violations of the same HIPAA provision during any calendar year (see below table). The lowest category of violation covers situations where the covered entity or business associate did not know, and by exercising reasonable diligence would not have known, of the HIPAA violation. The second lowest category of violation applies to violations due to reasonable cause and not to willful neglect. The third category applies to situations where the violation was due to willful neglect and was corrected within 30 days of when the covered entity or business associate knew, or should have known, of the violation. The fourth category applies to situations where the violation was due to willful neglect and not corrected within 30 days of when the covered entity or business associate knew, or should have known, of the violation.

Categories of HIPAA Violations and Corresponding Penalty Amounts

Violation Category	Penalty Per Violation	All such violations of an identical provision in a calendar year
Did not know	Between $100 and $50,000	$1.5 million
Reasonable cause	Between $1,000 and $50,000	$1.5 million
Willful neglect (timely corrected)	Between $10,000 and $50,000	$1.5 million
Willful neglect (not timely corrected)	$50,000	$1.5 million

The Final Rule modifies the definition of "reasonable cause" to mean "an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated [HIPAA], but in which the covered entity or business associate did not act with willful neglect." The Final Rule keeps the definition of "willful neglect" as the "conscious, intentional failure or reckless indifference to the obligation to comply" with HIPAA.

Counting Violations

In the preamble to the Final Rule, OCR states that, how it counts HIPAA violations for purposes of calculating a civil monetary penalty, varies depending on the circumstances surrounding the violation. OCR explains that where multiple individuals are affected by a HIPAA violation (e.g., a breach of unsecured PHI), it is anticipated that the number of identical HIPAA violations would be counted by the number of individuals affected. OCR also explained that, with respect to continuing violations (e.g., a lack of appropriate safeguards for a period of time), it is anticipated that the number of identical HIPAA violations would be counted on a per day basis (i.e., the number of days the covered entity or business associate did not have appropriate safeguards in place to protect the PHI). OCR notes that in many HIPAA breach cases, there would be both an impermissible use or disclosure, as well as a safeguards violation, for each of which OCR would be entitled to calculate a separate civil monetary penalty. Needless to say, the amount of civil monetary penalties can be quite substantial.

Factors Used to Determine a Penalty

The Final Rule lists the following five factors that OCR will consider in determining the amount of a civil monetary penalty:

- The nature and extent of the violation, including the number of individuals affected and the duration of the violation;
- The nature and extent of the harm resulting from the violation, including physical, financial, and reputational harm, and any hindrance to an individual's ability to obtain healthcare;

- The history of prior compliance with HIPAA, including whether the current violation is the same/similar to prior indications of noncompliance by the covered entity or business associate and their attempts to correct that noncompliance;
- The financial condition of the covered entity or business associate, including any financial difficulties that could have affected compliance and whether a civil monetary penalty could jeopardize the future provision of healthcare; and
- Such other matters as justice may require.

Agency Liability

The Final Rule makes covered entities and business associates liable for the acts of their business associate agents, regardless of whether the covered entity knew of the violation or had a compliant business associate agreement in place. According to OCR, the key factor in determining whether an agency relationship exists between a covered entity and its business associate, or between a business associate and its subcontractor, is the principal's right to control the agent's conduct in the course of performing a service on behalf of the principal. OCR observes that a business associate agent's conduct generally is within the scope of agency when its conduct occurs during the performance of the assigned work or incident to such work, regardless of whether the work was done carelessly, a mistake was made in the performance, or the business associate disregarded a covered entity's specific instruction. OCR further observes that, in contrast, a business associate agent's conduct generally is outside the scope of agency when its conduct is solely for its own benefit (or that of a third party), or it pursues a course of conduct not intended to serve any purpose of the covered entity.

RECOMMENDED ACTION ITEMS

Although covered entities and business associates have until September 23, 2013 to fully comply with the Final Rule, we recommend they begin preparing soon in light of the significant number of new or modified compliance obligations. In particular,

- Covered entities will need to revise, negotiate, and execute business associate agreements compliant with the Final Rule by September 23, 2013 to the extent they did not have business associate agreements in place as of January 25, 2013 that were HIPAA compliant; they have until September 22, 2014 to do so to the extent they had business associate agreements in place as of January 25, 2013 that were HIPAA compliant. At a minimum, covered entities will need to review their business associate agreements soon to determine which ones complied as of January 25, 2013 with HIPAA, and which ones did not as of that date, given that it could take a long time to finalize revised agreements.

- To the extent they have not done do, covered entities will need to draft, negotiate, and execute business associate agreements compliant with the Final Rule by September 23, 2013 with any individual or entity that maintains PHI on their behalf, including a data storage company. Covered entities also will need to enter into business associate agreements by September 23, 2013 with: (i) patient safety organizations; (ii) health information organizations, e-prescribing gateways, and others that provide data transmission services involving PHI to a covered entity and that require routine access to

such PHI; and (iii) vendors that offer a personal health record to an individual on behalf of a covered entity.

- Business associates that use subcontractors that create, receive, maintain, or transmit PHI on their behalf will need to draft, negotiate, and execute business associate agreements with them by September 23, 2013.

- The new categories of business associates, including subcontractors, will need to conduct a security risk assessment, implement a written HIPAA security plan, designate a security official, and create certain written HIPAA privacy policies by September 23, 2013. Existing business associates will also need to do this by September 23, 2013 to the extent they have not already done so. OCR has posted guidance on compliance with the HIPAA Security Rule found at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule, which may be helpful to business associates and facilitate their compliance efforts.

- Covered entities and business associates will need to perform a gap analysis to determine what HIPAA policies and procedures need to be revised to comply with the Final Rule, and then will need to revise them by September 23, 2013 based on the gap analysis.

- Covered entities will need to review any subsidized marketing arrangements to make sure they comply by September 23, 2013 with the new marketing restrictions requiring an individual's authorization.

- Covered entities will need to update their PHI access request forms by September 23, 2013 to comply with the Final Rule.

- Covered entities will need to determine if they are able to provide individuals with an electronic copy of PHI, and, if they cannot, to invest in technology that enables them to do so by September 23, 2013; business associates will need to do this if required in their business associate agreements.

- Covered entities may need to create and implement new patient authorization forms by September 23, 2013 to address marketing, sale of PHI, and fundraising communications.

- Healthcare providers will need to implement by September 23, 2013 a method to flag or make a notation in the record with respect to PHI that has been restricted in accordance with the Final Rule to ensure that such information is not inadvertently sent to or made accessible to a health plan for payment or healthcare operations purposes, such as audits by the health plan.

- Covered entities will need to revise their NPPs and ensure that they are properly posted and distributed by September 23, 2013.

- Covered entities and business associates will need to update by September 23, 2013 their breach notification policies and any tools concerning how to conduct a risk assessment to determine whether breach notification is required.

- Covered entities and business associates will need to update their HIPAA training materials and then train their workforce members (i.e., employees, volunteers, trainees, and other persons under their direct control) by September 23, 2013 to comply with HIPAA.

Given the breadth and potential penalties under the Final Rule, we have two additional recommendations concerning HIPAA. First, covered entities and business associates should review their data flows (i.e., the complete lifecycle of PHI that they create, receive, maintain, or transmit) and then perform an updated risk analysis based on that review, including a risk analysis of mobile devices. Covered entities and business associates will need to determine whether to encrypt these devices (see the firm's last Health Law Alert for the risks by not doing so). Second, covered entities and business associates should consider whether it would be cost-effective for them to purchase HIPAA liability insurance.

ADDITIONAL INFORMATION

Please feel free to contact us if you have any questions or need any assistance in complying with the Final Rule.