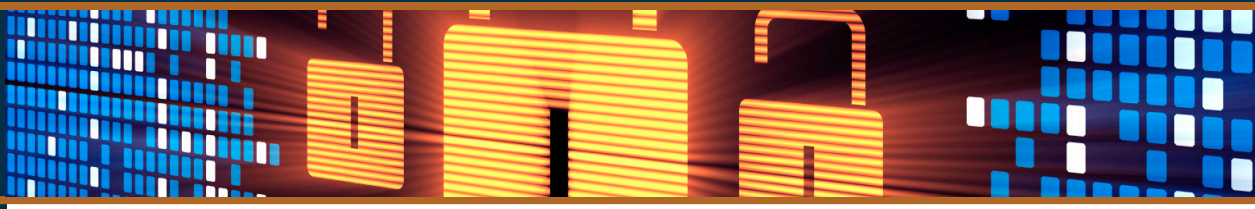
SHIPMAN & GOODWIN® LLP
COUNSELORS AT LAW

HEALTH LAW

February 12, 2013



Health Law Practice Group:

Joan W. Feldman
(860) 251-5104
jfeldman@goodwin.com

David M. Mack
(860) 251-5058
dmack@goodwin.com

Vincenzo Carannante
(860) 251-5096
vcarannante@goodwin.com

William J. Roberts
(860) 251-5051
wroberts@goodwin.com

Alex J. Hwang
(860) 251-5334
ahwang@goodwin.com

www.shipmangoodwin.com

HIPAA Final Rule

On January 17, 2013, the U.S. Department of Health and Human Services released the long-anticipated final rule modifying the Health Insurance Portability and Accountability Act's ("HIPAA") privacy, security, breach notification and enforcement rules. Covered entities and business associates will have until September 23, 2013 to comply with most of the major provisions of the final rule. This alert highlights and summarizes what we believe are some of the most pertinent provisions for our clients.

Modification of the Breach Notification Rules

First, and possibly most importantly, the Final Rule revises the definition of "breach" such that there is an automatic presumption that an impermissible use or disclosure of protected health information ("PHI") constitutes a breach. The Final Rule eliminates the prior harm standard which allowed entities to avoid notification if they could demonstrate that the breach posed no significant risk of financial, reputational or other harm to the affected individual. Now, under the Final Rule, notification may be avoided in connection with a breach if the entity can demonstrate through a risk assessment that there is a low probability that the PHI has been compromised[1]. The following factors need to be considered in determining whether the data has been compromised:

- 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.

---

1 Please note that breach notification may also be avoided if an exception is met. The definition of breach excludes (1) any unintentional acquisition, access, or use of PHI protected by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by HIPAA; (2) any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA; or (3) a disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

While HHS plans to provide entities with additional guidance related to risk assessments and frequently occurring breach scenarios, it is safe to say at this point that on the continuum of deciding whether parties need to make breach notifications, this Final Rule has definitely shifted the needle towards requiring notification.

Enforcement

The Final Rule retains the penalties for violations of HIPAA as proposed under the Health Information Technology for Economic and Clinical Health Act ("HITECH"), but makes clear that HHS has the discretion to set the specific penalty amount. When making its determination, HHS indicates that it may consider both the financial condition and size of the covered entity or business associate.

Type of Violation	Range for Each Type of Violation	Maximum Aggregate Penalty per Calendar Year for Each Type of Violation[2]
Lack of Knowledge	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect - Corrected	$10,000 - $50,000	$1,500,000
Willful Neglect - Not Corrected	$50,000 (minimum)	$1,500,000

The Final Rule also provides clarification on how HHS will count violations for purposes of assessing penalties. HHS anticipates that where multiple individuals are affected by an impermissible use or disclosure (such as in the case of a breach), the number of HIPAA violations would equal the number of individuals affected. For example, a breach of PHI affecting 300 individuals could be considered 300 separate HIPAA violations. With respect to continuing violations (such as a lack of appropriate safeguards for a period of time), HHS anticipates that the number of HIPAA violations would be counted on a per day basis. For example, a failure to have appropriate safeguards in place in violation of a certain HIPAA standard for 40 days could be considered 40 separate violations. HHS further notes that in many breach cases, HHS may find an impermissible use or disclosure as well as a safeguards violation, and HHS may calculate a separate civil monetary penalty for each. Thus, a breach that includes violations of multiple HIPAA requirements may result in penalties well above $1.5 million.

Business Associates and Subcontractors

Expanding the Definition of Business Associate. The Final Rule expands the definition of business associate to include the following:

2 Please note that this represents the maximum penalty amount per violation, but multiple violations are possible. Thus, there are separate limits for each rule violated under HIPAA.

- Health information organizations, e-prescribing gateways and other entities that provide data transmission services for covered entities and that require "routine" access to PHI (as opposed to no access or random access); and
- Entities that offer a personal health record to individuals on behalf of a covered entity.

Subcontractors. The Final Rule also expands the definition of business associate to include "subcontractors" (other than workforce members) that create, receive, maintain, or transmit PHI on behalf of a business associate. HIPAA now applies to all downstream subcontractors in the same manner as it applies to business associates that directly contract with or act on behalf of covered entities, and subcontractors now incur the same liability for noncompliance. Subcontractors must enter into business associate agreements with the business associate or upstream subcontractor that engaged the subcontractor.

Application of the Privacy and Security Rules to Business Associates. The Final Rule extends direct liability for compliance with HIPAA's Security Rule to business associates. Specifically, business associates must implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI that they receive, create, maintain or transmit on behalf of a covered entity. Such safeguards include, among others, performing a risk analysis, establishing a risk management program, designating a security official, preparing written policies and procedures, and conducting employee training. Business associates must also ensure that any subcontractor to whom they provide such information agrees to implement reasonable and appropriate safeguards to protect it.

The Final Rule also provides that any Privacy Rule limitation on how a covered entity may use or disclose PHI automatically extends to a business associate. The Final Rule also extends the following Privacy Rule requirements to business associates:

- HIPAA's minimum necessary rule applies to a business associate's use and disclosure of PHI, and its requests for PHI from another covered entity or business associate.
- Business associates are directly liable for (i) impermissible uses and disclosures of PHI, (ii) a failure to provide breach notification to the covered entity, (iii) a 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), (iv) a failure to disclose PHI where required by HHS to investigate or determine the business associate's compliance with HIPAA, and (v) a failure to provide an accounting of disclosures.

Please note, however, that the Final Rule does not apply all of the Privacy Rule's requirements to business associates. For example, business associates are not required to comply with other provisions of the Privacy Rule, such as providing a notice of privacy practices or designating a privacy official.

Vicarious Liability. The Final Rule clarifies that covered entities may be held liable for the acts of business associates and business associates are liable for the acts of subcontractors when the business associate or subcontractor is an agent[3]. While the Final Rule notes that each business associate or subcontractor relationship must be looked at individually, and must consider the totality of the circumstances, the Final Rule indicates that the "essential factor" for finding an agency relationship is the covered entity's right to control the business associate's conduct, regardless of the terms of the business associate agreement.

Revising Your Business Associate Agreements. In light of the Final Rule's modifications, covered entities and business associates should review their existing business associate agreements and revise as necessary. The Final Rule allows covered entities and business associates (and business associates and subcontractors) to continue to operate under existing business associate agreements until September 23, 2014.

Certain Specific Disclosures Permitted

Decedent's PHI. The Privacy Rule will no longer provide privacy protections for a decedent's PHI to the same extent and in the same manner as living individuals. Under the Final Rule, the PHI of individuals who have been deceased for more than 50 years will no longer be protected by the Privacy Rule at all. In addition, covered entities will be permitted to disclose PHI to a family member or other individual involved in the care of or payment of care of a decedent, unless this disclosure is inconsistent with a prior expressed preference of the decedent.

Proof of Immunization. The Final Rule permits a covered entity to disclose proof of immunization to a school where the law requires the school to have such information prior to admitting the student. Covered entities, however, must first obtain permission to do so (which may be written or oral permission) before disclosing such information.

Individual Rights

Covered Entities Must Honor Certain Requests to Restrict Disclosures to Health Plans. The Final Rule requires health care providers to honor requests to restrict disclosures to health plans (or the health plan's business associate) for purposes of carrying out payment or

3 The Final Rule adopts the Federal common law of agency to determine whether an agency relationship exists.

healthcare operations if the disclosure is not otherwise required by law and the PHI relates solely to a healthcare item or service for which the individual has paid the covered entity out of pocket and in full.

Patients Have Enhanced Rights to Electronic Copies of Records. The Final Rule establishes the right of patients to obtain a copy of their health records in electronic form when such information is maintained by a covered entity (or business associate) in electronic form in a designated record set (regardless of whether it is part of an electronic health record). Covered entities must provide the electronic copy in a machine readable format mutually agreed upon (e.g., MS Word or Excel, text, HTML, text-based PDF), but need not provide individuals with unlimited choices.

Enhanced Right of Access. The Final Rule provides individuals with the right to direct covered entities to transmit a copy of their records directly to a person or entity designated by the individual.

The Final Rule also tightens the time frame for providing access to records by eliminating the existing provision that allowed 60 days to provide access when records are maintained by the covered entity off-site. Under the new rule, covered entities must provide access to all paper and electronic PHI within 30 days of the individual's request with the option of a one-time 30-day extension available.

Research Authorizations

Compound Authorizations. The Privacy Rule prohibited covered entities from combining authorizations that condition treatment, payment, enrollment, or eligibility for benefits with authorizations for another purpose for which treatment, payment, enrollment or eligibility may not be conditioned. For example, research may include both treatment as part of the clinical trial and the banking of tissue and associated PHI. In such cases, the individual must sign an authorization for use of his or her PHI in order to receive the research-related treatment ("conditioned authorization"), but is free to sign or to not sign the authorization related to the tissue and data banking ("unconditioned authorization"). Previously, a covered entity was prohibited from using a single authorization form in this type of situation and was required to obtain two separate authorizations. The Final Rule now allows covered entities to combine conditioned and unconditioned authorizations for research purposes into a single form, provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities.

Authorizations for Future Research. HHS's prior Privacy Rule required that authorizations for research be study specific and not account for future research. Under the Final Rule, an authorization does not have to be study specific and may permit future research provided that the future research is adequately described such that the individual has a reasonable expectation that his or her PHI could be used or disclosed for such future research.

Marketing

The Final Rule requires a covered entity or business associate to obtain an individual's written authorization prior to using or disclosing that individual's PHI for marketing purposes, when such marketing involves the receipt of "financial remuneration"[4] by the covered entity or business associate. The Final Rule also clarifies that marketing includes all treatment communications made to an individual financed by a third party. However, the Final Rule maintains the following exceptions from HIPAA and HITECH for which no authorization is required:

- Face to face communications;
- Promotional gifts of nominal value;
- Refill reminders;
- Communications promoting health in general that do not promote a product or service from a particular provider; and
- Communications about government and government-sponsored programs.

When obtaining an individual's authorization for marketing communications involving financial remuneration, HHS permits the authorization to be specific to a particular product or service, the products or services of a particular third party or any marketing communications for which the covered entity receives financial remuneration.

Fundraising Communications

The Final Rule modifies the requirements regarding the types of information a covered entity may use or disclose for fundraising purposes and opt out methods that a covered entity may present to individuals who may not wish to receive such communications in the future.

Types of Information. The Final Rule expands the types of information covered entities may use or disclose to target "fundraising communications."[5] In addition to demographic information and the dates of health care provided to the individual, covered entities may

4 The Final Rule defines "financial remuneration" to include only payments made in exchange for making marketing communications. Financial remuneration does not include non-financial benefits, such as in-kind benefits.

5 A "fundraising communication" is a communication to an individual that is made by a covered entity, an institutionally related foundation, or a business associate on behalf of a covered entity, for the purpose of raising funds for the covered entity.

now utilize information regarding the department of service, the treating physician and outcome information for fundraising purposes.

Method and Scope of Opt Out. The Final Rule permits covered entities to select the methods individuals can use to opt out of receiving further fundraising communications, as long as the chosen methods do not impose an undue burden or more than a nominal cost on the individuals. According to HHS, the provision of a toll-free telephone number or an email address are viable opt out methods to present to individuals, while requiring individuals to write and send a letter asking not to receive further fundraising communications would constitute an undue burden. The Final Rule also allows covered entities to determine the scope of the opt out (whether the opt out applies to all future fundraising communications or just to a specific fundraising campaign) and to determine how individuals may opt back in if they so desire. The Final Rule prohibits the conditioning of treatment or payment on an individual's choice with respect to the receipt of fundraising communications.

Sale of PHI

The Final Rule prohibits the "sale of protected health information"[6] by a covered entity or business associate unless an authorization from the individual has been obtained. Any such authorization must state that the disclosure of PHI will result in remuneration to the covered entity. The term "remuneration" includes both financial and nonfinancial benefits. However, the Final Rule provides several exceptions to the authorization requirement where the exchange is for:

- Public health purposes;
- Research purposes, where a covered entity receives only a reasonable, cost-based fee to cover the cost to prepare and transmit the information for research purposes;
- Treatment and payment purposes;
- Disclosures related for sale, transfer and merger activity;
- Disclosures for business associate activities (that are otherwise in compliance with the Privacy Rule);
- Providing an individual with access to his or her PHI, where the fees charged are in accord with the Privacy Rule (a reasonable, cost-based fee);
- Purposes as required by law; and
- Purposes that otherwise fit into the requirements of the Privacy Rule.

6 "Sale of protected health information" is defined 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.

Revisions to Notices of Privacy Practices

Revising Your Notice of Privacy Practices. The Privacy Rule requires most covered entities to have and distribute a notice of privacy practices ("NPP") which describes the uses and disclosures of PHI it is permitted to make, its legal duties and privacy practices with respect to PHI, and the individual's rights concerning his or her PHI. The Final Rule requires several changes to a covered entity's NPP. NPPs must now:

- Describe certain uses and disclosures of PHI that require patient authorization, including those related to psychotherapy notes, marketing and the sale of PHI, as well as a statement that other uses and disclosures not described in the NPP will only be made with the individual's authorization;
- Inform individuals of their right to restrict a covered entity from disclosing PHI to health plans where the individual pays out of pocket in full for the health service or item to which the information relates;
- Include a statement regarding the right of affected individuals to be notified following a breach of unsecured PHI; and
- Include a statement that the covered entity may contact the individual for fundraising purposes and that the individual has a right to opt out of receiving such communications.

Notification of Revisions. Since HHS believes that these changes to NPPs constitute a material change, individuals must be notified of such revisions. The Final Rule requires that providers post their revised NPPs in a clear and prominent location. Providers must also have copies of the NPP available at the delivery site for individuals to request to take with them. Under the Final Rule, providers are only required to give a copy of the NPP to, and to obtain a good faith acknowledgment of receipt from, new patients.[7]

Compliance with the Final Rule will require changes to health care providers' HIPAA policies and procedures, business associate agreements and NPPs. If you have any questions about the Final Rule or would like assistance in complying with its requirements, please contact any of the members of the Shipman & Goodwin Health Law Practice Group.

7 The Final Rule also addresses notification requirements for health plans. Health plans that currently post their NPPs on their web sites must: (i) prominently post the material change or their revised NPP on their website by the compliance date of the Final Rule; and (ii) provide their revised NPP, or information about the material change and how to obtain their revised NPP, in their next annual mailing to individuals covered by the plan. Health plans that do not have web sites are required to provide the revised NPP, or information about the material change and how to obtain the revised NPP, to individuals covered by the plan within 60 days of the material revision to the NPP.

One Constitution Plaza
Hartford, CT 06103-1919
860-251-5000

300 Atlantic Street
Stamford, CT 06901-3522
203-324-8100

1133 Connecticut Avenue NW
Washington, DC 20036-4305
202-469-7750

289 Greenwich Avenue
Greenwich, CT 06830-6595
203-869-5600

12 Porter Street
Lakeville, CT 06039-1809
860-435-2539

www.shipmangoodwin.com

SHIPMAN & GOODWIN® LLP