SEIGFREID BINGHAM

Health Care Quarterly

SPRING 2013

IN THIS ISSUE:

911 Main Street
Suite 2800
Kansas City, MO 64105
seigfreidbingham.com
P: 816-421-4460
F: 816-474-3447

HHS Issues Long-Awaited HIPAA Regulations Under the HITECH Act

By Heath Hoobing, hhoobing@seigfreidbingham.com

On January 25, 2013, the Department of Health and Human Services (HHS) published final regulations that implement changes to HIPAA's Privacy and Security Rules. The changes originated from the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted nearly four years earlier, but generally have been on hold pending the issuance of these regulations. Although the new regulations leave most of the prior rules in place, the changes made by the new regulations will impact every health care provider and provider of services to the health care industry. This newsletter summarizes the most significant changes made by the HITECH Act and the new regulations, which include new obligations and liabilities for Business Associates and their subcontractors, the methodology for determining whether a breach of protected health information (PHI) has occurred, and restrictions on the sale of PHI and the use or disclosure of PHI for marketing or fundraising purposes.

Our firm has reviewed the new HIPAA regulations thoroughly, and we are currently updating our model HIPAA Business Associate Agreement, Notice of Privacy Practices, and Compliance Guide to ensure their conformity with the new regulations. After we complete this process over the next several weeks, we will publish an alert highlighting the key changes that must be made to amend Business Associate Agreements and the Notice of Privacy Practices to ensure continued compliance.

Additionally, our firm can help you:

- Determine how you could potentially reduce the risk and amount of fines or penalties that could be assessed if your Business Associate or its subcontractor is found to be non-compliant with HIPAA;
- Conduct a HIPAA risk assessment, which is critical to ensure your continued compliance with HIPAA following any change in your business practices or information technology, or a potential breach of PHI;
- Analyze the issues confronting the health care industry due to the incorporation of agency principles from employment law in allocating liabilities for HIPAA violations;
- Determine whether an unauthorized use or disclosure of PHI is a breach under the new definition that would require you to take corrective action; and
- Determine how you may now use PHI for marketing or fundraising purposes.

Seigfreid Bingham's health care attorneys would be happy to assist you with any questions you may have regarding the new HIPAA regulations. We also can review your HIPAA compliance plan and other HIPAA documents or address any other HIPAA-related concerns so that you can spend more time serving your patients and clients and less time worrying about compliance with HIPAA.

Updating HIPAA Compliance Plans and Documents Under the New HIPAA-HITECH Omnibus Rule Regulations

By John Fuchs, johnf@seigfreidbingham.com and Kyle Ritchie, kritchie@seigfreidbingham.com

Every entity that participates in the health care sector, whether an independent health care provider, a hospital system, a health care IT vendor, or a health plan, must reevaluate its HIPAA compliance plan in light of the changes enacted by the new HIPAA regulations which went into effect on March 26, 2013. The new regulations, often called the HIPAA-HITECH Omnibus Rule, amends HIPAA's governing regulations to make them compliant with the HITECH Act, including raising the potential level of enforcement penalties to $1.5 million per year per section violated. All Covered Entities, Business Associates, and Business Associate subcontractors need to consider which documents or practices require updating to maintain their HIPAA compliance as the HIPAA requirements continue to evolve with the changing landscape of health care, technology, and privacy.

Likely the most critical changes enacted by the new HIPAA regulations are the redefinition and expansion of Business Associates' and their subcontractors' HIPAA responsibilities and the use of agency law to allocate liability and knowledge of HIPAA violations. Subject to certain exceptions, a Business Associate is now defined as a person who creates, receives, maintains, or transmits protected health information in connection with a HIPAA-regulated function or activity, or provides legal, actuarial, accounting, consulting, data aggregation, management, or similar services that involve the disclosure of protected health information. In other words, a Covered Entity's business universe is full of potential Business Associates. Until HHS issues further guidance, it appears that the addition of the word "maintains" to the definition means that cloud storage service providers are subject to HIPAA if they maintain protected health information for a Covered Entity or Business Associate.

Every participant in the health care market will need to reevaluate their relationships with other health care businesses to ensure that the proper agreements govern their relationship and that they have correctly allocated the compliance responsibilities between the parties as intended. Entities that provide services to Business Associates and were not previously directly subject to HIPAA may now be "subcontractors" under the regulations. Business Associates are required to enter into Business Associate Agreements with all of their subcontractors that handle protected health information. Covered Entities are not required to have any agreements with a Business Associate's subcontractors, but the Business Associate Agreement between a Covered Entity and a Business Associate must require that the Business Associate ensures their subcontractors' compliance through the Business Associate's agreements with its subcontractors.

The use of agency law to allocate liability and knowledge of violations means that Covered Entities may be responsible for HIPAA violations by their Business Associates if the Covered Entity has the authority to control the conduct of the Business Associate, other than by termination of a contract. This determination will be made based on the potential control available and will not depend on whether the parties agree that their relationship is not an agency relationship. Further compounding these issues, if a Business Associate is determined to be an agent of a Covered Entity then any knowledge of a HIPAA breach by the Business Associate is imputed to the Covered Entity as of the day the Business Associate learns of the violation. This means that the clock for providing any required notifications to the affected individuals, the Secretary of Health and Human Services, and potentially the media starts ticking as soon as the Business Associate or subcontractor learns of a breach. All of the above rules also apply to the liability of Business Associates with respect to their Business Associate subcontractors. The good news is that the new regulations clarify that a Covered Entity or Business Associate is generally not responsible for a breach by its Business Associates if they are not agents. In light of these changes, it is essential that every Covered Entity and Business Associate know which of their Business Associates and/or subcontractors are their agents to determine both the desired level of indemnification provided by their contracts and the timeframe in which any breach must be reported.

Every business or provider subject to HIPAA must be in compliance with the new rules by **September 23, 2013**. The documents which must be revised and redistributed by all entities subject to HIPAA include all Business Associate Agreements, the Notice of Privacy Practices, and any related compliance plan documents or guidance. Business Associate Agreements (or other contracts that contain the required Business Associate provisions) that were entered into before January 25, 2013, and are not renewed or modified between March 26 and September 23, 2013, are grandfathered and do not need to be updated until September 22, 2014 (see the Compliance Timeline Chart on page 7). However, if a Business Associate Agreement (or other contract) is renewed or modified on or after September 23, 2013, the Business Associate Agreement or other contract must be updated to comply with the new rules at the time of renewal or modification.

New HIPAA Final Regulations Amending Breach Definition and Civil Monetary Penalties

By Mark Opara, mopara@seigfreidbingham.com

The HITECH Act requires Covered Entities to notify affected individuals of any breach of unsecured protected health information. The HITECH Act defined "breach" as the "unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information," subject to certain exceptions for unintentional or inadvertent disclosures.

Then, in an interim final rule, which was effective Sept. 23, 2009, HHS defined "compromises the security or privacy of the protected health information" to mean "poses a significant risk of financial, reputational or other harm to the individual."

Effective September 23, 2013, the new HIPAA regulations have changed the definition of breach to no longer include the "significant risk of harm" standard. The existence of a breach now depends on whether there is a "low probability" that the protected health information has been "compromised" based on the following four factors:

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

Under the new regulations, any acquisition, access, use or disclosure of protected health information not permitted by the Privacy Rule is *presumed* to be a breach unless the Covered Entity or Business Associate demonstrates the low probability of compromise by performing a risk assessment utilizing at least the four factors stated above. While the new regulations do not explain what it means for information to be "compromised," the new definition appears to remove much of the discretion a Covered Entity may have had under the prior definition in determining the existence of a breach based on a significant risk of harm. Additionally, it is now clear that the Covered Entity or Business Associate bears the burden of demonstrating that the information is not "compromised" in order to avoid determining that a breach has occurred.

Practically, this does not appear to affect the result of a breach analysis in most cases. The primary exception is that if the recipient of information in a potential breach is unknown, then it appears impossible to demonstrate a low probability of compromise, whereas under the former rule a Covered Entity may have been able to find no substantial risk of harm to the affected individuals in some cases. Considering this new definition, all Covered Entities and Business Associates should consider encrypting any protected health information stored on mobile devices, such as laptops, tablets, and cell phones, so that if the device is lost or stolen, there will be a low risk of compromise and thereby limit this potential source of a breach.

The new regulations also raise the liability for HIPAA violations to $100-$50,000 per violation with a $1.5 million annual cap and clarify the method by which HHS will calculate the penalties for such violations. Furthermore, the new regulations significantly expand liability by subjecting Business Associates and their downstream subcontractors to direct liability for certain HIPAA violations.

The new regulations allow HHS to treat an ongoing violation of a provision or a violation affecting multiple individuals as multiple violations. Under the prior regulations, it was uncertain how HHS would apply a violation of a single provision that affected multiple individuals or continued over time without being cured.

(Continued on page 4)

(Continued from page 3)

The new regulations provide that HHS will apply the number of violations of a single Privacy Rule provision deriving from a breach based on the number of individuals whose information was disclosed. HHS could then render a fine up to $50,000 for each disclosure, multiplied by the number of individuals affected, subject to a cap of $1.5 million. Furthermore, the same breach could be the result of a separate violation for failure to implement adequate physical security of protected health information that is continued over a period of time. In that instance, the regulations permit HHS to count the number of times the provision was violated based on the number of days the violation continued. Based on the culpability level of the individual or entity, HHS could therefore impose a separate $50,000 fine for each violation of the Security Rule, multiplied by the number of days the violation occurred, subject to a separate cap of $1.5 million for the calendar year. Thus, in the above example, the individual or entity could face up to $3 million in potential liability.

New Rules Regarding Use/Disclosure of PHI for Fundraising Purposes

By Milos Jekic, mjekic@seigfreidbingham.com

This Article summarizes the changes made by the recently released HIPAA regulations regarding the use/disclosure of protected health information (PHI) for fundraising purposes. Specifically, the Article examines (i) the categories of PHI that can be used/disclosed for fundraising purposes and (ii) the requirements imposed in connection with the use/disclosure of PHI for fundraising purposes.

CATEGORIES OF PHI THAT CAN BE USED/DISCLOSED FOR FUNDRAISING PURPOSES

The new regulations significantly expand the types of PHI that may be used or disclosed for fundraising purposes. Under the new regulations, the categories of PHI that can be used or disclosed include:

- Demographic information relating to the individual, including name, address, other contact information, age, gender, and date of birth;
- Dates of health care provided to the individual;
- Department-of-service information, which includes information about the general department of treatment, such as cardiology, oncology, or pediatrics;
- Treating physician;
- Outcome information, which includes information regarding the death of the patient or any sub-optimal result of treatment or services; and
- Health-insurance status.

Covered Entities must still apply the minimum-necessary standard to ensure that only the minimum amount of PHI necessary to accomplish the intended purpose is used or disclosed.

REQUIREMENTS IN CONNECTION WITH USE/DISCLOSURE OF PHI FOR FUNDRAISING PURPOSES

The new regulations also expand the requirements imposed upon a Covered Entity that uses PHI for fundraising purposes. Under the new regulations, Covered Entities that use or disclose PHI for fundraising purposes are subject to the following requirements:

- PHI may not be used or disclosed for fundraising purposes unless the Covered Entity informs individuals in its Notice of Privacy Practices that it might contact them to raise funds and that they have a right to opt out of receiving such communications.
- With each fundraising communication made to an individual, whether made in writing or over the phone, the Covered Entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications.
- Covered Entities are free to provide individuals with the choice of opting out of all future fundraising communications or just campaign-specific communications. Whatever method is employed, the communication should clearly inform individuals of their options and any consequences of electing to opt out of further fundraising communications.

(Continued on page 5)

(Continued from page 4)

- The method for an individual to elect not to receive further fundraising communications cannot cause the individual to incur an undue burden or more than a nominal cost. The new regulations encourage Covered Entities to consider the use of a toll-free phone number, an e-mail address, or similar opt-out mechanism that would provide individuals with a simple, quick, and inexpensive way to opt out of receiving future communications. Requiring that individuals opt out of further fundraising communications by simply mailing a pre-printed, pre-paid postcard would not constitute an undue burden under the new regulations and is an appropriate alternative to the use of a phone number or e-mail address. Conversely, requiring individuals to write a letter to opt out constitutes an undue burden.
- A Covered Entity may choose to provide individuals with the opportunity to select their preferred method for receiving fundraising communications. If an individual elects to opt out of future fundraising communications, then the opt out is effective for all forms of fundraising communications and the individual must be removed from all such lists.
- The Covered Entity may not make fundraising communications to an individual where the individual has elected not to receive such communications. However, the Covered Entity may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.
- The Covered Entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

New Rules Regarding Sale of PHI and Use/Disclosure of PHI for Marketing Purposes

By Milos Jekic, mjekic@seigfreidbingham.com

The recently released HIPAA regulations make numerous changes to the HIPAA regulatory framework. This Article summarizes the changes regarding the sale of protected health information (PHI) and the use/disclosure of PHI for marketing purposes.

SALE OF PHI

Under the new regulations, a Covered Entity must obtain an authorization from the individual for any disclosure of the individual's PHI that constitutes a "sale of protected health information." Such authorization must state that the disclosure will result in remuneration to the Covered Entity or Business Associate. "Sale of protected health information" means 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. Remuneration includes both financial and non-financial, in-kind benefits.

"Sale of protected health information" does not include a disclosure of PHI for the following purposes:

- 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 other Business Associate, where the only remuneration provided is for the performance of such activities;
- To an individual when requested in connection with the individual's right of access to PHI or right to obtain an accounting of the disclosures of PHI;
- When required by law; and
- For any other permissible purpose, 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.

(Continued on page 6)

(Continued from page 5)

USE/DISCLOSURE OF PHI FOR MARKETING PURPOSES

Covered Entities must obtain an authorization from an individual before using or disclosing the individual's PHI in connection with "marketing" a product or service. "Marketing" means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. The foregoing rule is subject to several exceptions. It does not apply to communication in the form of (i) a face-to-face communication made to the individual or (ii) a promotional gift of nominal value.

In addition, this rule does not apply to certain types of communications that are excluded from the definition of "marketing." Marketing does not include a communication made for the following treatment and health care operations purposes:

- For treatment of an individual by a health care provider;
- To describe a health-related product or service that is provided by, or included in a plan of benefits of, the Covered Entity making the communication, including communications about the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health-plan enrollee that add value to, but are not part of, a plan of benefits; or
- For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions.

Prior to the HITECH Act, these exclusions applied regardless of whether the Covered Entity received any benefits in connection with the use or disclosure of PHI. Under the new regulations, the above exclusions do not apply if a Covered Entity receives any financial remuneration in exchange for making the communication.

The new regulations also provide that marketing does not include a communication made to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, but only if (i) no financial remuneration is received by the Covered Entity or (ii) any financial remuneration that is received by the Covered Entity in exchange for making the communication is reasonably related to the Covered Entity's cost of making the communication.

"Financial remuneration" means a direct or indirect payment from or on behalf of a third party whose product or service is being described. "Direct or indirect payment" does not include a payment for the treatment of an individual. Unlike the definition of "remuneration" discussed above in the context of sale of PHI, the definition of "financial remuneration" in the context of marketing does not include non-financial benefits, such as in-kind benefits, which may be provided to a Covered Entity in exchange for making a communication about a product or service. Only payments made in exchange for making such communications are included within the definition.

Permissible costs for which a Covered Entity may receive financial remuneration under this exception are those that cover only the costs of labor, supplies, and postage to make the communication. The financial remuneration a Covered Entity receives in exchange for making the communication cannot generate a profit or include payment for other costs.

Synthesizing the above-described general standard and its exceptions, the net result is that Covered Entities must generally obtain an authorization from the individual before using or disclosing the individual's PHI for marketing communications that involve the receipt of financial remuneration. The authorization must disclose the fact that the Covered Entity is receiving financial remuneration from a third party. Prior authorization is also required where a Business Associate (including a subcontractor), as opposed to the Covered Entity itself, receives financial remuneration from a third party in exchange for making a communication about a product or service.

Compliance Timeline

Date:	*Description:*
March 26, 2013	Effective date of changes to the HIPAA enforcement provisions, including civil penalties
September 23, 2013	Notices of Privacy Practices must be amended and redistributed
September 23, 2013	Non-grandfathered Business Associate Agreements must be amended
September 23, 2013	Business Associates must have a Business Associate Agreement with each subcontractor who is a Business Associate
September 22, 2014	Final date to amend grandfathered Business Associate Agreements between Covered Entities and Business Associates. A Business Associate Agreement is grandfathered if it was executed prior to January 25, 2013 and was not amended or renewed between January 25 and September 23, 2013.

Health Care Group Members

Mark R. Thompson, Co-Chair
Mark H. Gilgus
John M. Neyens
John G. Peryam
Christopher J. Stewart
Tim Grasser
John C. Fuchs
Joseph L. Hiersteiner, Co-Chair
Lori A. Beam
Angie S. Armenta
Heath W. Hoobing
Mark U. Opara
Milos J. Jekic
Kyle D. Ritchie