Summary of New HIPAA Final Privacy Regulations

On January 17, 2013, the Department of Health and Human Services released final regulations which provided sweeping changes to the rules update under privacy, security, enforcement, and breach notification requirements of the Health Insurance Portability and Accountability Act ("HIPAA"), the Health Information Technology for Economic Health ("HITECH") and Genetic Information Nondiscrimination Act ("GINA") Group health plans and business associates are required to comply with the regulations by September 23, 2013, unless otherwise stated in the regulations. With respect to the requirements on breaches of unsecured Protected Health Information ("PHI"), group health plans must still comply with the September 23, 2009 date. The following is a summary of the important changes under these final regulations.

1. Business Associates

Definition of Business Associate

Several updates and clarifications to the HIPAA definition of Business Associates ("BA") have been included.

A person or entity becomes a BA by (i) meeting the definition of a BA and (ii) creating, receiving, maintaining, or transmitting PHI on behalf of a covered entity. Whether or not such person or entity has contracted with the covered entity and/or has entered into a Business Associate Agreement ("BAA") is not determinative. Additionally, the type of PHI involved in the transaction does not matter – information is considered PHI if the information is related to a covered entity.

The definition of BAs also include:

- health information organizations;
- e-prescribing gateways;
- other entities that provide data transmission services with respect to PHI to a covered entity and that require routine access to PHI;
- entities that offers a personal health record to one or more individuals on behalf of a covered entity; and
- entities that maintain PHI, whether or not the entities actually review the PHI.

Subcontractors of BAs

The HIPAA's BA provisions also apply to BAs' subcontractors (persons or entities that provide services to a BA which involves PHI to fulfill its contractual duties) if the subcontractors create, receive, maintain, or transmit PHI on behalf of BAs. Group health plans are not required to enter into Business Associate Agreements ("BAAs") with subcontractors, but the BAA must contain provisions that BAs will ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the BA agree to the same HIPAA restrictions, conditions, and requirements that apply to the BA.

Additional Clarifications Regarding Bas

- Banking and financial institutions are not BAs with respect to payment process activities, as identified in § 1179 of HIPAA, but if the bank or financial institution's scope of activities exceeds the payment process activities, it will be considered a BA.

- Patient safety activities were added to the list of functions that may be undertaken as a BA and were added to the definition of health care operations.

- An insurer of a health plan product or insurance policy that is purchased by a covered entity is not a BA of the covered entity just by providing the insurance or product. In order to be considered a BA, the insurer must perform a function that involves PHI.

Direct Liability

BAs are now directly liable for complying with certain HIPAA privacy and security rules:

- Impermissible use and disclosure of PHI
- Failure to provide breach notification to a covered entity
- Failure to disclose PHI when required
- Failure to provide access to electronic PHI to an individual, his/her designee or a covered entity
- Failure to provide to a covered entity an accounting of disclosures
- Failure to comply with HIPAA security rules contained in 45 C.F.R. §§ 164.306, 164.308, 164.310, 164.312, and 164.314
- Failure to comply with the requirements relating to policies, procedures and documentation requirements of 45 C.F.R. § 164.316
- Failure to establish BAAs with subcontractors

2. Business Associate Agreements ("BAA")

All Business Associate Agreements must be amended to include:

- Provisions requiring BAs to comply with the HIPAA security rule
- Provisions requiring BAs to report breaches involving unsecured PHI to covered entities
- Provisions requiring BAs to obtain satisfactory assurances that subcontracts agree to comply with the underlying BAA's conditions and restrictions as applied to PHI

Additionally, the final regulations do remove the requirement that BAAs include a provision that required covered entities to report to the Department of Health and Human Services when a BA was out-of-compliance, was not able to cure the breach, and it was not possible to terminate the BAA between the covered entity and the BA.

The final regulations also provide for a "grandfathered" transition period for updating BAAs. If a HIPAA-compliant BAA was in effect prior to January 25, 2013 and is not renewed or modified between March 26, 2013, and September 23, 2013, the covered entity and BA may continue to operate under the current BAA for up to **one year past** the final regulation compliance date. That is, the BAA does not have to be amended until the earlier of: (1) the date the BAA is renewed or modified on or after September 23, 20133 or (2) September 22, 2014. This extension for compliance also applies to BAAs that contain automatic renewal provisions.

3. Notice of Privacy Practices

Notices of Privacy Practices ("NPP") must now be amended to include the following information (in addition to the existing HIPAA requirements):

- A statement indicating 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;
- A statement that an individual has a right to or will receive notifications of breaches of his or her unsecured PHI;
- If the plan intends to use or disclose PHI for underwriting purposes, a statement that the plan is prohibited from using or disclosing PHI that is genetic information of an individual for such purposes; and
- If the plan intends to contact an individual to raise funds for the plan, a statement regarding fundraising communications and an individual's right to opt out of receiving such communications.

For group health plans that post the NPP on their websites, the final regulations require that these plans must prominently post the changes or a revised Notice of Privacy Practices on websites by the September 23, 2013 compliance date; and provide the revised Notices of Privacy Practices, or information about the changes and how to obtain the revised Notices of Privacy Practices, in their next annual mailings to individuals then covered by the plans, such as at the beginning of the plan year or during open enrollment.

4. Breach Notification

<u>Definition of Breach</u>

The definition of what constitutes a "breach" has been changed. Breach is now defined as the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the security or privacy of such information. However, the final regulations made no change to the existing exceptions to the definition of breach.

With the change to the definition of breach, the previously used risk of harm standard has been replaced with the rule that, unless one of the enumerated exceptions is applicable, an unauthorized use or disclosure of PHI is presumed to be a breach. To overcome the presumption, a covered entity or BA must show that there is a "low probability that the PHI has been compromised."

In support of this, the final regulations also identified four factors that must be evaluated by a covered entity or BA when determining whether PHI has been compromised:

1. What is the nature and extent of the PHI involved in the potential breach,
2. Who was the unauthorized user or recipient of the PHI,
3. Was the PHI actually received or viewed by the unauthorized user or recipient, and
4. To what extent has the breached PHI been mitigated.

The above four factors of the risk assessment are not determinative. Other factors may also need to be considered, depending on the individual circumstances of the breach. The risk assessment performed and conclusions reached by the covered entity or BA should be documented.

Additionally, the definition of breach has been changed by removing the exception for limited data sets that do not contain any dates of birth and zip codes.

Notice Requirements

Only a few changes have made to the breach notice requirements. These include:

- A covered entity must notify the Department of Health and Human Services of all breaches affecting fewer than 500 individuals not later than 60 days after the end of the calendar year in which the breach was discovered rather than when the breach occurred
- Covered entities may delegate responsibility for breach notifications to a BA provided the BAA provisions provide that the BA has the same obligations that the covered entity has under the final regulations
- The plan is not required to incur costs to print or run a media notice, when it must provide notice of a breach to the media (i.e., breaches involving 500+ individuals in a state or jurisdiction). Also, media outlets are not obligated to print or run information about breaches when they receive notifications about them.
- The plan must provide notice within 60 days after the plan discovers the breach (rather than 60 days after the breach occurred), when the notice of a breach affects fewer than 500 individuals.

For this purpose, discovery means the first day on which an employee, officer other agent of the covered entity or BA knows or should know by exercising reasonable diligence of the breach.

5. Use and Disclosure of PHI

Use and Disclosure of PHI for Marketing Purposes

Individuals must now provide authorizations for certain communications where covered entities use or disclose PHI and receive financial remuneration for making the communications from a third party whose product or service is being marketed.
The Department of Health and Human Services clarified that remuneration related to marketing communications must be from or on behalf of the entity whose product or service is being described as well as it being in exchange for making the communication itself. Even if a BA, rather than the covered entity, receives the payment, the communication would be considered a marketing communication.

A covered entity must obtain an individual's authorization prior to using or disclosing PHI about the individual for marketing purpose other than the following:

- treatment or health care operations activities that are made face-to-face, or
- The provision of a promotional gift of nominal value to the individual.

The definition of marketing does not include:

- refill reminders or other communications about a drug that is currently prescribed for the individual, as long as the financial remuneration received is reasonably related to the cost of making the communication
- promoting health in general, not promoting a specific product or service
- information related to government and government-sponsored programs

Use of PHI for Fundraising Purposes

If a covered entity (or a BA), uses an individual's PHI for purposes of raising funds, the communication's recipient must be provided with a "clear and conspicuous" opportunity to opt out of receiving any further fundraising communications. The method for "opting out" is left up to the covered entity to determine. However, the opt-out process may not create undue burden or more than nominal cost for the individual.

The use and disclosure of the following types of PHI can be used for fundraising:

- Demographic information relating to an individual,
- Dates of health care provided to an individual,
- Department of service information,
- Outcome information, and
- Health insurance status

However, the rule that when using PHI to make fundraising communications, the minimum necessary standard still applies and only the minimum amount of PHI

necessary to accomplish the intended purpose may be used or disclosed is still applicable.

Prohibition on Sale of PHI

A covered entity or BA is only allowed to receive remuneration (direct or indirect) in exchange for the disclosure of PHI if an individual's authorization is granted. The authorization must state that direct or indirect remuneration is being received in exchange for the PHI, unless an allowed exception applies. Sale of protected health information is defined as the disclosure of PHI by a covered entity or BA, where the entity or BA directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI. The exceptions to the prohibition of the sale of PHI are:

- For public health purposes
- For treatment of the individual and payment purposes.
- For the sale, transfer, merger or consolidation of all or part of a covered entity and for related due diligence purposes if the recipient of the PHI is or will become a covered entity
- For research purposes, if the remuneration is cost-based
- Services rendered by a BAA under a BAA at the specific request of the covered entity, as long as the remuneration is cost-based
- Providing an individual with access to the individual's PHI
- As required by law
- For any other purpose permitted by HIPAA

Other Changes to Use and Disclosure of PHI

PHI stored in electronic devices such as photocopiers, fax machines, and other devices is now subject to the Privacy and Security Rules.

Covered entities are now permitted to disclose decedents' PHI to family members and others who were involved in decedents' care or payment for care prior to death, unless the covered entities know that such disclosure would be inconsistent with the decedents' prior expressed wishes. If such disclosure will be allowed by the covered entity, it must be limited to PHI relevant to the family members or other persons' involvement in the decedents' health care or payment for health care.

Additionally, a covered entity may disclose proof of immunizations to schools in states that have laws that require the school to have such information prior to admitting a student. Although written authorization for the disclosure is not required, it is encouraged.

6. Changes to Patient Rights

Right to Access Protected Health Information

If individuals requests electronic copies of PHI that are maintained electronically in one or more designated record sets, covered entities must now provide access to the information in the electronic form and format requested by the individual, if readily producible.

If not readily producible, covered entities must provide the PHI in a readable electronic form and format which is agreed to by the covered entities and the individual, such as Word, Excel, text, HTML, or text-based PDF. Additionally, the final regulations provide:

- A plan must respond to such a request within 30 days of the request, with a one-time 30-day extension when necessary. If a plan takes the 30-day extension, it must provide written notice to the individual of the reasons for delay and the expected date for completing the request.
- If an individual declines any readily producible electronic format, the plan must provide a hard copy as an option.
- A plan can require individuals to make these requests for PHI in writing.
- A plan is not required to scan paper documents to provide electronic copies.
- If requested, a plan must transmit the copy of PHI directly to another person designated by the individual who is the subject of the PHI. If an individual directs the plan to send a copy of PHI to another person, the request must be in writing, signed by the individual, and clearly identify the designated person and where to send the PHI. The plan must implement reasonable policies and procedures to verify the identity of any person who requests PHI and implement reasonable safeguards to protect the information used or disclosed.
- With respect to PHI from an electronic health record in electronic form, a plan cannot charge more than labor costs in responding to an individual's request. These costs may include skilled technical staff time spent to create and copy the electronic file or time spent preparing and explanation or summary of the PHI, if appropriate. A plan also can charge for the cost of supplies (such as CDs or USB drives) for creating the copy of PHI, if the individual requests the electronic copy on portable media, and associated postage.

Restrictions on Disclosures by Health Plans

The processes surrounding the requirement that covered entities must comply with an individual's request to restrict disclosure of PHI to a health plan if certain conditions are met have been clarified. Under the final regulations:

- Health providers are not required to maintain separate medical records when a request to restrict disclosure is made, but they are required to use some method to identify which portions of the medical records are subject to the restriction request.

- If a restriction is requested where payment is pending, health providers must either make reasonable efforts at resolving the payment issues before disclosing PHI or should request payment in full at the time of the requested restriction.
- If an individual requests a restriction, it is the individual's responsibility – not the health providers – to notify any other providers who might be impacted.
- HMO contractual requirements do not negate a provider's responsibility to adhere to a request to restrict disclosures.

7. Penalties

Consequences of Noncompliance

The final regulations significantly increase covered entities and BAs potential exposure to civil monetary penalties and creates uncertain risk. First, covered entities and BAs will be liable under federal common law of the acts of their agents.

Next, the assessment of penalties will be left to fact specific analyses and the Department of Health and Human Services' discretion. There are four categories of HIPAAA violations that reflect increasing levels of culpabilities accompanied by four tiers of significantly increased monetary penalties. These include:

Tier 1: For violations in which it is established that the covered entity of BA did not know and, by exercising reasonable diligence, would not have known that the covered entity violated a provision, an amount not less than $100 or more than $50,000 for each violation

Tier 2: For a violation in which it is established that the violation was due to reasonable cause and not to willful neglect, an amount not less than $1000 or more than $50,000 for each violation

Tier 3: For a violation in which it is established that the violation was due to willful neglect and was timely corrected, an amount not less than $10,000 or more than $50,000 for each violation

Tier 4: For a violation in which it is established that the violation was due to willful neglect and was not timely corrected, an amount not less than $50,000 for each violation

A penalty for violations of the same tier will not exceed $1.5 million in a calendar year, but multiple violations of multiple requirements may be subject to the maximum penalty of $1.5 million times the number of requirements violated.

The maximum penalty amount will not necessarily be levied in all cases. There will be a determination based on factors including but not limited to: the nature and extent of the violation; the harm resulting from the violation; prior offenses or compliance of the entity involved; and the financial condition of the entity.

The final regulations provide insight into the application of penalties. In the case of a breach that affects multiple individuals, the number of violations will be based on the number of individuals affected. In the case of a breach that is continuous over a period of time, the number of violations will be based on the number of days that the entity did not have the breached information sufficiently protected. In the case of a breach involving violations of two or more provisions, a separate calculation may be made for each provision breached.

Increased penalty amounts may be levied if the violation due to willful neglect is not corrected within 30 days. Under the final regulations, for violations involving willful neglect, additional penalties may be assessed if the entity does not correct within 30 days. The 30 days begins to run when the entity first has actual or constructive knowledge of a violation due to willful neglect.

8. GINA Implementation

The Department of Health and Human Services' proposals have be adopted to:

- Provide that genetic information is considered health information for purposes of HIPAA privacy rules and therefore subject to HIPAA privacy requirements;
- Prohibit all health plans that are subject to HIPAA privacy rules from using or disclosing PHI that is genetic information for underwriting purposes (except with regard to insurance issuers of long term care policies);
- Revise the HIPAA requirements relating to Notices of Privacy Practices for health plans that perform underwriting;
- Make conforming changes to definitions and other provisions of the HIPAA privacy rules; and
- Make technical corrections.

For a copy of the final regulations, please click on the link below:

https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the

515-225