

MEMORANDUM

February 17, 2009

**HITECH Act of Stimulus Bill
Imposes More Stringent HIPAA Privacy & Security Requirements,
Appropriates Funds for Health Information Technology**

H.R. 1, the new stimulus package that was signed by President Obama on February 17, 2009, imposes significant new HIPAA privacy and security requirements on health plans, business associates, and other vendors of personal health records. The bill also includes appropriations for health information technology (HIT) and new HIT requirements for the government sector (or businesses who have government contracts). The HIT and HIPAA requirements fall under the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

Among the new requirements, described in more detail below, are a duty to notify each individual in the event of a security breach, the extension of direct penalties to business associates, additional access and accounting requirements, and stricter criminal and civil enforcement. Most of the HIPAA privacy and security requirements go into effect one year from enactment, although some provisions (as noted) have shorter or longer deadlines.

Below we highlight the major new requirements of the legislation. (Note that references to "HIPAA" are to the HIPAA Privacy & Security Rules, 45 CFR Parts 160-164.)

A. Extension of HIPAA Privacy & Security Rules to Business Associates

Under current law, the HIPAA privacy and security rules apply to covered entities, which are defined as health plans, health care providers, and health care clearinghouses. If a health plan uses a service provider, such as a third party administrator, it must have a business associate contract with the service provider, but the business associate is not directly regulated by HIPAA or subject to HIPAA's civil and criminal penalties (rather, it may be contractually liable through its business associate contract).

The new law generally would apply the HIPAA privacy and security requirements to business associates in the same manner as they apply to covered entities. This means that a business associate would be subject to the same penalties as the covered entity. The new law also provides that business associate agreements must be revised to include any new privacy or security requirements of the legislation.

In addition, any entity that provides data transmission services to a covered entity would be considered a business associate under the new law (and so directly liable under HIPAA as well). The statute indicates that this includes PHR vendors and health information exchanges.

These new requirements are effective 12 months after enactment.

B. Duty to Notify in Case of Breach

Currently, if there is a privacy or security breach, HIPAA requires a health plan to mitigate any harmful effect, which could include reviewing its privacy and security procedures, imposing sanctions on workforce members, or documenting its response to a complaint. There is no express requirement that the health plan notify individuals whose information may have been breached (there are state duty to notify laws, but these generally do not apply to health plans).

The new law would require a covered entity to notify each individual in the event their protected health information (PHI) was breached. The notification must be made within 60 days of discovery (or the date the breach reasonably should have been discovered) and must describe the circumstances of the breach, including the date of the breach and date of discovery, the type of PHI involved, steps individuals should take to protect themselves, and steps the covered entity is taking to mitigate harm and protect against future breaches. If the breach is by a business associate, the business associate must notify the covered entity, including the identity of each individual involved.

The notice must be made by first class mail or electronic mail "if specified as a preference" by the individual. If more than 500 individuals in a state or jurisdiction are involved, the covered entity must provide notice to "prominent media outlets" serving the state or jurisdiction. The covered entity also must notify the Secretary of Health and Human Services – immediately for breaches involving 500 or more individuals and on an annual basis for other breaches. The Secretary will list breaches involving more than 500 individuals on its website.

It appears that the duty to notify rule only will apply where the covered entity or business associate has "unsecured" PHI – that is, PHI that is not secured under standards to be set by the Secretary. The new law does not specifically indicate that encryption is required in order for PHI to be considered "secure." The law directs the Secretary to issue guidance within 60 days of enactment specifying which technologies will be considered secure.

The Secretary is required to issue interim final regulations governing the duty to notify within 180 days of enactment. The duty to notify requirement would apply to breaches discovered on or after 30 days of these regulations being issued.

A similar provision applies to vendors of personal health records (PHRs). These vendors also are required to notify individuals or the media (if applicable) upon a breach of an unsecured PHR. The FTC is required to issue interim final regulations governing a PHR vendor's duty to notify within 180 days of enactment. The duty to notify requirement would apply to breaches discovered on or after 30 days of these regulations being issued.

C. Accounting for Treatment, Payment, & Health Care Operations Disclosures

The HIPAA privacy rules currently allow an individual to request an accounting of disclosures of their PHI for the previous six years, subject to some exceptions. One of these exceptions is for routine disclosures for the purpose of treatment, payment, or health care operations, which are defined terms under the regulations. Instead, the covered entity is required to issue a general privacy notice that explains what types of disclosures are made for these more routine purposes.

The new law would require a covered entity that maintains an "electronic health record" to include routine disclosures for treatment, payment, or health care operations (TPO) in its accounting list. The TPO accounting would be limited to 3 years (accounting for other disclosures would remain 6 years, as under the current rule).

An "electronic health record" is defined as an electronic record of health-related information on an individual that is created, gathered, managed, or consulted by authorized health care clinicians and staff. It is not clear how this definition and new requirement would apply to health plans, which typically do hold claims records that are created by health care providers, either who treat a participant or whom the plan has consulted in deciding a claim.

For electronic health records held by a covered entity as of January 1, 2009, the TPO accounting requirement would apply to TPO disclosures on or after January 1, 2014. For electronic health records acquired by a covered entity after January 1, 2009, the TPO accounting requirement would apply to TPO disclosures on or after January 1, 2011. The law provides that the Secretary may delay these dates, but no later than 2016 and 2013, respectively.

D. Remuneration for Exchange of PHI or Marketing Communications

Currently, the HIPAA privacy rules require a covered entity to obtain an individual's authorization for certain "marketing" purposes. The authorization must state whether the covered entity is receiving direct or indirect remuneration for the communication. The regulations define "marketing" as a communication that encourages the recipient to purchase or use a product or service and lists several exceptions that are not considered marketing (*e.g.*, communications about other benefits under the health plan). However, if the communication falls under the definition of "health care operations," rather than "marketing," the covered entity is not required to obtain authorization or disclose possible remuneration.

The new law would clarify that, in order to fall under the definition of "health care operations" (so no authorization is required), the communication must meet the exceptions under the "marketing" definition, and the covered entity must not receive direct or indirect remuneration in connection with the communication. The law provides an exception where the communication describes only a drug or biologic that is currently being prescribed and any remuneration is "reasonable." This provision would apply 12 months after enactment.

The new law also prohibits direct or indirect remuneration for any exchange of PHI (even under payment or health care operations), unless the individual has so authorized. The authorization must specify whether the covered entity may further exchange the PHI for remuneration. The new law provides exceptions where the PHI is exchanged for public health activities, research, treatment, the sale of the covered entity, services under a business associate contract, providing the individual with a copy of his or her PHI, or as determined by the Secretary in regulations. The Secretary is required to issue regulations on this rule within 18 months of enactment, and the new prohibition is effective 6 months following final regulations.

E. Access to Electronic PHI

HIPAA currently gives individuals the right to access their PHI from a covered entity. The covered entity generally must respond to the request within 60 days and may charge a cost-based fee for copying costs, labor, and postage.

The new law would provide that, where the covered entity holds an "electronic health record" (as defined above), the individual must be able to request their information under the right to access requirement in electronic form. The covered entity only may charge labor costs. In addition, an individual may direct the covered entity to transmit a copy of his or electronic health record directly to an entity or person designated by the individual. These provisions would be effective 12 months after enactment.

F. Right to Restrict Disclosures for Payment & Health Care Operations

Currently, HIPAA allows individuals a right to request that a covered entity not disclose their PHI, even for purposes of routine treatment, payment, or health care operations. However, the covered entity is not required to agree to the restriction.

The new law would require the covered entity to agree to the restriction when an individual requests to restrict disclosures to a health plan for payment and health care operations, where services for treatment have been paid out of pocket in full. This appears to mean that if an individual has paid out of pocket for a certain treatment, the provider or another plan would not be permitted to disclose this information to another health plan, if requested by the individual (*e.g.*, for underwriting purposes).

G. Enforcement

HIPAA currently allows the Secretary of Health and Human Services to impose a civil penalty of \$100 per violation of the HIPAA privacy and security rules, with a maximum of \$25,000 for violations of an identical requirement during a calendar year. The statute provides exceptions where the covered entity did not know of a violation or the failure was due to reasonable cause and corrected within 30 days. The Secretary also has the authority to perform compliance reviews and investigate complaints. In addition, the Department of Justice has authority to bring criminal penalties ranging from \$50,000 and one year of imprisonment for wrongful disclosure of PHI to \$250,000 and 10 years of imprisonment for offenses committed for commercial gain.

Civil Penalties

The new law would require the Secretary to periodically audit covered entities and to formally investigate a covered entity where a complaint has been received. The Secretary would be limited in when he or she could bring voluntary corrective action (as generally is the case now) to circumstances where covered entity did not know of the violation (and by exercising due diligence would not have known).

The new law also would increase the civil penalty amounts and distinguish by type of violation, as follows:

- No Knowledge - Where a person does not know (and by exercising due diligence would not have known) of a violation, the minimum penalty is \$100 per violation, with a cap of \$25,000 for violations of an identical requirement during a calendar year; the maximum penalty is \$50,000 per violation, with a cap of \$1.5 million for violations of an identical requirement during a calendar year;
- Reasonable Cause - Where a violation is due to "reasonable cause," the minimum penalty is \$1,000 per violation, with a cap of \$100,000 for violations of an identical requirement during a calendar year; the maximum penalty is \$50,000 per violation, with a cap of \$1.5 million for violations of an identical requirement during a calendar year; and
- Willful Neglect - Where violation is due to "willful neglect," the minimum penalty is \$10,000 per violation, with a cap of \$250,000 for violations of an identical requirement during a calendar year; the maximum penalty is \$50,000 per violation, with a cap of \$1.5 million for violations of an identical requirement during a calendar year.

The bill provides that these penalties may not apply if the violation is corrected within 30 days of the date the person knew of the violation (or should have known, by exercising reasonable diligence).

The new civil penalty amounts would apply to violations after the date of enactment. The other procedural enforcement provisions would apply to penalties imposed 24 months after enactment. The Secretary is required to issue regulations related to these enforcement provisions within 18 months of enactment.

The new law also requires the GAO to study methodologies for allowing a percentage of civil penalties to be paid to harmed individuals. The Department of Health and Human Services must establish such a methodology within 3 years of enactment.

Criminal Penalties

Criminal penalty amounts would remain the same, but the Secretary would have authority to bring criminal actions, along with the Department of Justice. In addition, the new law clarifies that criminal action may be brought against any individual who wrongfully discloses PHI, not just the covered entity itself or employees of the covered entity.

Actions by State Attorneys General

In addition, state Attorneys General will have authority to bring civil actions against a covered entity to enjoin violations and obtain damages on behalf of the residents of that state of up to \$100 per violation, with a maximum of \$25,000 for violations of an identical requirement during a calendar year. The action must be brought in federal district court and may not be brought if the Secretary already has instituted action. This provision applies to violations occurring any time after the date of enactment.

Application to Business Associates

Since other provisions of the new law extend HIPAA directly to business associates, these new penalty provisions would apply to business associates in the same manner as covered entities.

H. Health Information Technology (HIT) Provisions

The new law also seeks to vastly expand use of health information technology (HIT) and appropriates \$250 million for Fiscal Year 2009 for implementing the new HIT provisions. The law requires the Secretary to appoint a National Coordinator for the Office of the National Coordinator for Health Information Technology (ONCHIT). The National Coordinator would be responsible for coordinating HIT policies and programs, developing a voluntary HIT certification program, and setting milestones for utilization of Electronic Health Records (EHRs) for each person in the United States by 2014. The new law also would provide a variety of incentives to promote use of EHRs, telemedicine, and clinical data repositories.

The law would require federal agencies that implement, acquire, or upgrade HIT systems to use systems and products that meet the standards adopted by the Secretary. In addition, health care payers and providers that contract with the federal government must use HIT systems and products that meet the required standards as well. The new law expressly provides that these standards otherwise would be voluntary for private entities.

Author: Christy Tinnes

We will provide updates on further developments. In the meantime, if you have any questions, please contact your regular Groom attorney or any of the Health and Welfare Practice Group attorneys listed below:

Jon W. Breyfogle	jwb@groom.com	(202) 861-6641
Jenifer A. Cromwell	jac@groom.com	(202) 861-6329
Thomas F. Fitzgerald	tff@groom.com	(202) 861-6621
Debbie G. Leung	dgl@groom.com	(202) 861-2601
Christine L. Keller	clk@groom.com	(202) 861-9371
Heather E. Meade	hem@groom.com	(202) 861-0179
William F. Sweetnam	wfs@groom.com	(202) 861-5427
Christy A. Tinnes	cat@groom.com	(202) 861-6603
Donald G. Willis	dgw@groom.com	(202) 861-6332
Brigen L. Winters	blw@groom.com	(202) 861- 6618