



## **HITECH Act Expands HIPAA Privacy and Security Rules** **Executive Summary**

On February 17<sup>th</sup>, President Obama signed the American Recovery and Reinvestment Act of 2009 (the stimulus bill). A portion of the bill created the Health Information Technology for Economic and Clinical Health Act (the HITECH Act).

**Electronic Health Record Financial Incentives and Grants for Health Information Exchange:** The HITECH Act provides substantial Medicare and Medicaid incentives for hospitals and physicians to adopt electronic health records (EHRs) and provides grants for the development of health information exchange (HIE). These incentives and grants will provide the needed support for many health care providers to adopt technology necessary to improve the quality and efficient of patient care. Stay tuned for a future memorandum from Coppersmith Gordon on these EHR incentives and HIE grants.

**Changes to the HIPAA Privacy and Security Rules:** The HITECH Act also substantially expands the HIPAA Privacy and Security Rules and increases the penalties for violations of HIPAA. This memorandum discusses the new requirements that:

- Apply the HIPAA privacy and security requirements directly to business associates;
- Establish mandatory federal security breach reporting requirements for HIPAA covered entities and their business associates;
- Create new privacy requirements for HIPAA covered entities and their business associates, including new accounting requirements for EHR, restrictions on marketing and fundraising, and other developments; and
- Establish new criminal and civil penalties for noncompliance and new enforcement responsibilities.

### **Next steps:**

- ***Be prepared:*** Review this memorandum with your legal counsel and HIPAA Privacy and Security officers. While most of the new requirements are not effective immediately, it will take some time to determine where your policies and procedures and HIPAA training will need to be updated.
- ***Watch for new rules and guidance:*** Monitor the development of HHS regulations and guidance documents issued under the HITECH Act. Anticipated publication dates for these rules and guidance documents are noted below.
- ***Respond promptly to compliance issues:*** Respond immediately to any information about potential HIPAA violations within your organization. The new penalty provisions are enforceable immediately against covered entities – with new enforcement authority by State Attorneys General. This makes it more important than ever to ensure compliance.

## PRIVACY AND SECURITY REQUIREMENTS FOR BUSINESS ASSOCIATES

**The HITECH Act applies the HIPAA Privacy and Security Rules – and their penalties – to HIPAA business associates.**

*Security Requirements.* The HITECH Act substantially expands the scope of the HIPAA Privacy and Security Rule by applying most of the rules' provisions to business associates. Section 13401 of the Act requires individuals and entities acting as "business associates" of HIPAA covered entities to comply with the HIPAA Security Rule provisions on:

- Administrative safeguards (45 C.F.R. § 164.308)
- Physical safeguards (45 C.F.R. § 164.310)
- Technical safeguards (45 C.F.R. § 164.312)
- Policies and documentation (45 C.F.R. § 164.316), and
- The new security breach reporting requirement (see below).

While business associates presently have to comply with their business associate contractual requirements to have adequate administrative, physical and technical safeguards in place to protect health information received from covered entities, most of those business associate contracts did not impose specific security requirements and did not require business associates to have written policies and documentation of security safeguards in place.

*Privacy Requirements.* Section 13404 of the Act requires HIPAA business associates to comply with 45 C.F.R. § 164.504(e) (which sets forth the privacy terms required in HIPAA business associate agreements). While these contract obligations have always been enforceable by covered entities, they are now enforceable by the government through HIPAA. Business associates also are required to comply with the additional privacy requirements imposed by the Act described below.

*HIEs and RHIOs Are Business Associates.* Section 13408 of the Act specifies that certain entities are business associates if they require access to protected health information (PHI) on a routine basis, including Health Information Exchange Organizations, Regional Health Information Organizations, e-prescribing gateways, or a vendor that contracts with a covered entity to allow that covered entity to offer a personal health record to patients as part of its EHR.

*Criminal and Civil Penalties.* Finally, the Act makes HIPAA's criminal and civil penalties (42 U.S.C. § 1320d-5 and § 1320d-6) applicable to business associates. This will raise the stakes considerably for individuals and entities that perform services on behalf of HIPAA covered entities, and will put more pressure on the determination of whether an individual or entity is a "business associate" under HIPAA's convoluted definition of business associate (at 45 C.F.R. § 160.103).

*Effect on Existing Business Associate Agreements.* We do not think the Act requires covered entities to redo all of their existing business associate agreements. Section 13401 provides that

the “additional requirements of this title that relate to security” (security breach reporting) shall also be incorporated into the business associate agreement between the business associate and the covered entity”; Section 13404 has similar language with regard to the “additional requirements of this title that relate to privacy.” We think the statute automatically makes these additional provisions part of existing business associate agreements by operation of law, and does not require amendment of existing business associate agreements. Nonetheless, we recommend that HIPAA covered entities establish a process to educate their business associates on the new requirements and amend existing agreements as necessary to protect the interests of the covered entities.

Compliance Date. The basic requirements are effective one year from the date of the enactment of the Act, or February 17, 2010. The security breach reporting requirement and some of the additional privacy requirements have different effective date provisions, as described below.

## SECURITY BREACH REPORTING REQUIREMENTS

**The HITECH Act creates a new security breach reporting requirement for HIPAA covered entities and their business associates.**

Section 13402 of the Act creates a new federal security breach reporting requirement for HIPAA covered entities and their business associates. This section requires a covered entity that “accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses **unsecured protected health information**” to “notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such **breach**.”

This new requirement hinges on two important definitions:

- **Unsecured protected health information:** Section 13402(h) defines this term as PHI that is not secured through the use of a technology or methodology specified by HHS guidance. HHS is required to issue annual guidance by May 16, 2009 regarding the technologies and methodologies that render PHI “unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.” This means that, if a covered entity or business associate does not comply with this HHS guidance (and each subsequent HHS guidance issued annually), it will have “unsecured PHI.” If HHS does not issue guidance, then covered entities and business associates must comply with standards issued by an ANSI-accredited organization. If a covered entity or business associate complies with HHS guidance (or other standards in the absence of HHS guidance), then its information is not “unsecured PHI” and a breach would not be reportable.
- **Breach:** Section 13400 defines “breach” as follows:
  - (A) In general.--The term “breach” means 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.

(B) Exceptions.--The term "breach" does not include--

- (i) any unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate if--
  - (I) such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; and
  - (II) such information is not further acquired, accessed, used, or disclosed by any person;

or

- (ii) any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at same facility;

and

- (iii) any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

This means that unintentional or inadvertent access to information in an EHR by employees, agents or medical staff members is not a reportable breach unless that person further uses or discloses the PHI in an unauthorized manner. It also will not apply to disclosures to other unauthorized persons if they would not reasonably have been able to retain such information.

Notice Requirements. The Act contains rigorous notification requirements.

- *Individuals notified; timing:* Covered entities must notify "each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach" without unreasonable delay and in no case later than 60 days of discovery of the breach by the covered entity or its business associate (unless there is a law enforcement request for delay).
- *Manner and form of notice:* Notice must be made by first-class mail (or email if specified by an individual). If there is insufficient or out-of-date contact information, a covered entity must do a "substitute form of notice"; if there are more than 10

- individuals affected, the entity must do a conspicuous Web site posting or notice in major print or broadcast media.
- *Notice to the media:* If more than 500 residents of the State are involved, the entity must provide notice to “prominent media outlets.”
  - *Self-disclosure to HHS:* If more than 500 residents of the State are involved, the entity must provide immediate notice to HHS. If fewer than 500 residents are involved, the entity must log the breach and disclose it to HHS in an annual report.
  - *Content of notice:* The regulations require the notice to individuals to contain a description of what happened and the unsecured PHI involved steps for individuals to protect themselves, a description of the covered entity efforts to investigate, mitigate and prevent further breaches, and contact information.

A business associate is not required to provide notice of breach to the individual. Rather, a business associate must notify the covered entity of a breach, along with identification of each affected individual.

*Other Entities Subject to the New Security Breach Reporting Requirements.* The new security breach reporting requirements apply to other non-HIPAA covered entities as well. Vendors of personal health records (PHR), entities that provide products or services through the Web site of PHR vendors, and entities that access or send information to a PHR are required to notify each citizen or resident of the United States of a breach of security where their “unsecured PHR identifiable information” was acquired by an unauthorized person as a result of the breach. These entities also are required to notify the Federal Trade Commission of the breach. The failure to comply will be an “unfair and deceptive act or practice” under the FTC Act.

*Compliance Date.* HHS and FTC must issue interim final regulations to implement this section within 180 days, or by August 16, 2009. Entities are required to comply with the Act’s security breach reporting requirements for breaches that are discovered 30 days after HHS and FTC issue regulations.

*Continued Application of State Security Breach Reporting Statutes.* State security breach reporting statutes continue to apply if the state reporting requirements are more stringent than the federal provisions. Section 13421 of the Act applies the HIPAA state law preemption standards at 42 U.S.C. § 1320d-7. This supersedes any “contrary” provision of State law, except when the state law is “more stringent” than HIPAA. State laws are generally “more stringent” if they provide greater rights to individuals or greater privacy protection.

## ADDITIONAL PRIVACY REQUIREMENTS

**The HITECH Act creates new privacy requirements for HIPAA covered entities and their business associates.**

*Request for Restrictions on Disclosures to Health Plans.* The HIPAA Privacy Rule currently permits an individual to ask a covered entity to restrict the usual manner in which the covered entity makes disclosures for treatment, payment and health care operations. However, the covered entity is not required to agree to the request. Section 13405(a) of the HITECH Act now requires

a covered entity to grant an individual's request not to disclose PHI to a health plan for a health care item or service where the individual has paid in full out of pocket. This provision is effective one year from the date of the enactment of the Act, or February 17, 2010. This provision also applies to business associates.

Minimum Necessary. The HIPAA Privacy Rule currently requires a covered entity to restrict its disclosures to the "minimum necessary" amount of information required for the purpose of the disclosure. The rule permits covered entities to rely on a request by other covered entities and its business associates as being the minimum necessary. Section 13405(b) of the new statute requires the covered entity to make the determination of minimum necessary, rather than relying on others to make that decision. The statute also provides that a "Limited Data Set" (information that has been partially de-identified) always meets the minimum necessary standard.

This provision is effective one year from the date of the enactment of the Act, or February 17, 2010. This provision is applicable to business associates. However, HHS is instructed to issue guidance on what constitutes "minimum necessary" within 18 months, at which point this statutory provision sunsets, and the HHS guidance will control.

New Electronic Health Record Provisions for Accounting for Disclosures of PHI for Treatment, Payment and Health Care Operations. The HIPAA Privacy Rule currently requires covered entities to provide an "accounting" of disclosures of PHI to individuals at their request, with various exceptions, including disclosures that are made for treatment, payment and health care operations. Section 13405(c) of the new statute provides that disclosures made through an EHR for treatment, payment and health care operations purposes must be included in the accounting, but information is limited to three years of disclosure information (rather than six). Covered entities will have the choice of including information about electronic disclosures by their business associates, or providing a list of their business associates, which then would be required to provide the accounting directly to individuals.

HHS is required to issue regulations on the new accounting requirements within six months. The statute instructs HHS to require only information that takes into account the interests of individuals in learning the circumstances under which their PHI is disclosed and to consider the administrative burden in writing these regulations.

If a covered entity acquired an EHR before January 1, 2009, the HHS regulations will be effective for disclosures made from the EHR starting on January 1, 2014. If a covered entity acquires an EHR after January 1, 2009, the regulations will apply to disclosures starting on January 1, 2011. In the regulations, HHS is permitted to provide an additional two years for compliance.

No Payment for PHI. The HIPAA Privacy Standards currently permit a covered entity to receive payment for a disclosure of PHI where that disclosure is permitted by the regulations (such as for the entity's health care operations, for research, and other activities). Section 13405(d) of the new statute now prohibits indirect and direct remuneration for a disclosure of PHI without the individual's authorization. The authorization document must also explain whether PHI can be

further exchanged for remuneration by the downstream entity receiving the PHI. The statute contains several exceptions where a covered entity is still permitted to receive remuneration for disclosures:

- For public health activities,
- For research, where the price charged reflects the costs of preparation and transmittal of the data,
- For treatment,
- For the sale, merger or transfer of the covered entity (which is a health care operation),
- To a business associate to perform functions for the covered entity,
- To an individual who wants copies of his or her PHI, and
- That fall within any future regulatory exceptions.

HHS is required to issue regulations related to this requirement within 18 months. In developing these regulations, the statute charges HHS with evaluating the cap on prices charged for data in research and with examining public health disclosures. The statutory requirements apply six months after HHS issues final regulations. This restriction on disclosures applies to business associates.

*Individual Access to PHI.* The HIPAA Privacy Rule currently requires covered entities to provide access to individuals of PHI in a “designated record set” with some exceptions, in the “form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual.” Section 13405(e) of the new statute requires covered entities that maintain PHI in EHRs to provide access in electronic format, and to transmit a copy of that PHI to an entity or person designated by the individual, such as another provider or a personal health record vendor. This provision applies in one year, on February 17, 2010. This applies to business associates.

*Marketing.* The HIPAA Privacy Rule requires an individual’s authorization to use PHI for “marketing” for most purposes. While marketing is defined as “a communication about a product or service that encourages recipients of the communication to purchase or use the product or service,” the definition of marketing excludes communications:

- To describe a health-related product or service (or payment for such 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
- For treatment of the individual, or

- For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

Section 13406(a) of the new statute prohibits a covered entity from obtaining direct or indirect payment for these types of communications without an authorization, except if the payment is for treatment or other limited circumstances. This provision applies in one year, on February 17, 2010, and applies to business associates.

*Fundraising.* The HIPAA Privacy Rule currently permits covered entities to use limited PHI about individuals (demographic information and dates of service) – such as patient lists – to do fundraising. It requires a covered entity to include in all fundraising materials a description of how the individual may opt out of receiving any further fundraising communications, and to make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications. Section 13406(b) of the new law mirrors the existing opt-out requirement, but makes an opt-out the equivalent of an authorization revocation. The practical effect of this change is to increase the importance of ensuring an individual's opt-out is honored. This provision applies in one year, on February 17, 2010. This applies to business associates.

## PENALTIES AND ENFORCEMENT

**The HITECH Act increases the penalties for HIPAA covered entities and business associates that violate HIPAA.**

*Criminal Penalties.* Section 13409 of the Act provides that the HIPAA criminal penalties apply to individuals who without authorization obtain or disclose individually identifiable health information that is maintained by a HIPAA covered entity. This provision clarifies that an individual does not need to be a HIPAA covered entity to be subject to the criminal penalties in 42 U.S.C. § 1320d-6(a). This provision applies in one year, on February 17, 2010.

*Civil Penalties.* Section 13410 makes a variety of changes to the civil penalty provisions. First, the Act adds that noncompliance for willful neglect requires HHS to formally investigate a complaint and to impose a civil penalty. HHS is required to implement regulations, and these statutory amendments will be effective in 24 months.

The section also requires civil penalties collected for privacy or security violations to go to the HHS Office for Civil Rights to fund enforcement. The Government Accountability Office is also directed to issue a report on sharing a percentage of these penalties with individuals who are harmed, and HHS is directed to issue regulations within three years.

The Act also increases the amount of civil penalties from the present \$100 per violation (up to \$25,000 per identical violation), to the following tiered civil penalties:

- *If the person did not know (and by exercising reasonable diligence would not have known) that such person violated a provision*, the civil penalty is between \$100 - \$50,000 for each

- violation, up to a total of \$25,000-\$1,500,000 for all violations of an identical requirement;
- *If the violation was due to reasonable cause and not to willful neglect*, the civil penalty is between \$1,000 - \$50,000 for each violation, up to a total of \$100,000-\$1,500,000 for all violations of an identical requirement;
  - *If the violation was due to willful neglect*, the civil penalty is between \$10,000 - \$50,000 for each violation, up to a total of \$250,000-\$1,500,000 for all violations of an identical requirement if the violation was corrected during the 30 day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred. If the violation is not corrected within 30 days, the penalties increase to \$50,000 for each violation, up to a total of \$1,500,000 for all violations of an identical requirement.

*Enforcement Authority to State Attorneys General.* Section 13410(e) gives enforcement authority to State Attorneys General to enforce the HIPAA Privacy and Security Rules, where an Attorney General has “reason to believe that an interest of one or more of the residents of that State has been or is threatened or adversely affected by any person who violates a provision of this part.” State Attorneys General are authorized to bring a civil action to enjoin a violation or to obtain statutory damages on behalf of those residents. These statutory damages are calculated by multiplying the number of violations by \$100, up to \$25,000 for violations of each identical requirement. The Act also permits states to seek the award of attorneys’ fees.

*Audits.* Finally, the Act requires HHS to do periodic audits to ensure that covered entities and their business associates are complying with the HIPAA regulations.

These new enforcement penalties are applicable immediately.

\*\*\*

For any questions about the HITECH Act, please contact Kristen Rosati at 602-381-5464 or [krosati@cgsblaw.com](mailto:krosati@cgsblaw.com) or other members of the CGSB Health Care Law Group.

**The CGSB Health Care Law Group**

Beth Schermer: 602.381.5462, [bschermer@cgsblaw.com](mailto:bschermer@cgsblaw.com)

Karen Owens: 602.381.5463, [kowens@cgsblaw.com](mailto:kowens@cgsblaw.com)

Julie Nelson: 602.381.5465, [jnelson@cgsblaw.com](mailto:jnelson@cgsblaw.com)

Kristen Rosati : 602.381.5464, [krosati@cgsblaw.com](mailto:krosati@cgsblaw.com)

Joel Wakefield : 602.381.5480, [jwakefield@cgsblaw.com](mailto:jwakefield@cgsblaw.com)

Mayan Tahan : 602.381.5475, [mtahan@cgsblaw.com](mailto:mtahan@cgsblaw.com)

*This Client Alert is published by Coppersmith Gordon Schermer & Brockelman PLC for general information purposes only, and should not be construed as legal advice or a legal opinion regarding any particular facts or circumstances. For advice and information concerning fact-specific situations and any specific legal questions you may have, please consult the attorney with whom you regularly work or contact one of our attorneys listed above.*