



Changes to HIPAA Usher in New Era of Electronic Health Data

As part of the American Recovery and Reinvestment Act (ARRA) signed into law by President Obama on February 17, 2009, changes have been made to privacy and security requirements applicable to protected health information (PHI) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These changes were added in connection with a \$19 billion appropriation designed to advance health information technology and incentivize the use of electronic health data and information. While most of the changes are not effective immediately, covered entities, business associates and certain other types of entities should become familiar with these changes and take steps to comply with the new requirements.

BACKGROUND

HIPAA mandated the development of standards governing the privacy and security of certain protected health information. Final HIPAA privacy standards were issued by the Department of Health and Human Services (HHS) in August 2002, and compliance with these standards was required by April 14, 2003 (or April 14, 2004 for small health plans). Final security standards were issued by HHS in February 2003, and compliance with these requirements was generally required by April 21, 2005 (April 21, 2006 for small health plans). The privacy and security standards apply to "covered entities," which include group health plans, certain health care providers and health care clearinghouses. Among other things, the standards require covered entities to enter into agreements with their third-party service providers, referred to as "business associates," obliging them to agree to comply with certain privacy and security requirements.

NEW PRIVACY AND SECURITY REQUIREMENTS

ARRA imposes new requirements on both covered entities and business associates. These new requirements and their effective dates are outlined below:

Covered Entities

Breach Notification. Notify each individual whose "unsecured" PHI is breached.

- Make the notification without unreasonable delay and in any event within 60 days of discovery (or within 60 days of the date the breach should have been discovered).
• Make the notification by first-class mail, or by electronic mail "if specified as a preference" by the individual, and include the following information:
- Circumstances of the breach
- Date of the breach
- Date of the discovery
- Type of PHI involved
- Steps individuals should take to protect themselves
- Steps the covered entity is taking to mitigate harm and to protect against future breaches
- How the individual can obtain additional information about the breach



- Maintain a log of breaches that affect fewer than 500 individuals and report such breaches annually to HHS. If a breach affects 500 or more individuals, notify HHS immediately. HHS will post information about breaches affecting more than 500 individuals.
- Notify “prominent media outlets” serving a state or jurisdiction if the breach affects more than 500 residents of that state or jurisdiction.
- HHS is required to issue guidance on what is “secure” and “unsecure” by April 18, 2009. Absent guidance, “unsecured” PHI means that which is not secured by a technology standard that renders the PHI unusable, unreadable or indecipherable and that is endorsed by a standards-developing organization accredited by the American National Standards Institute.
- HHS is also required to issue interim final regulations on the security breach notification requirements by August 16, 2009. The requirements will become effective 30 days after the regulations are published.

*Prohibition on Sale of PHI.* Do not accept remuneration for PHI without the individual’s authorization (unless it is to recoup the costs of providing data to a public health official, to a researcher, or to the individual herself, or meets certain other exceptions).

- HHS must issue regulations by August 18, 2010. These provisions become effective six months after the date of the final regulations.

*Restriction on Marketing.* Follow these guidelines when sending marketing materials on or after February 17, 2010:

- Do not send an individual marketing materials *and get paid for it*, unless she authorizes it or she is taking the medicine being marketed.
- Do not send an individual marketing materials *for free*, unless she authorizes it or the communication is made for certain purposes (*e.g.*, to describe a product available in the health plan or to recommend alternative health care options).

*Satisfaction of “Minimum Necessary.”* Whenever sufficient to carry out the purpose for which PHI is being used or disclosed, use or disclose PHI in the form of a “limited data set.” This requirement is satisfied by removing names, street addresses, social security numbers and other identifiers.

- This provision is effective for disclosures on and after February 17, 2010 and until HHS issues regulations on what constitutes “minimum necessary” information. These regulations are required to be issued by August 18, 2010.
- This does not affect the current “minimum necessary” requirement under HIPAA, which requires that covered entities use reasonable efforts to limit PHI to the “minimum necessary” when using or disclosing PHI, except in certain circumstances.

*Individuals’ Rights.*

- If maintaining “electronic health records” (EHRs), provide an individual (or her designee) upon request with a copy of the information in such EHR in electronic format. This provision becomes effective on February 17, 2010. Note, an EHR is an electronic record of health-related information on an individual that is created, gathered, managed and consulted by health care clinicians and staff.
- If using or maintaining EHRs, provide an individual upon request with an accounting of disclosures of the information in her EHR during the last three years, including disclosures made for treatment, payment or health care operations.
  - For covered entities who acquired an EHR after January 1, 2009, this requirement will apply to disclosures from such record made on or after January 1, 2011.



- For covered entities who acquired an EHR on or before January 1, 2009, this requirement will apply to disclosures from such a record made on or after January 1, 2014.
- Effective on and after February 17, 2010, honor the request of an individual *not* to disclose to her health plan the PHI related to a particular treatment *if* the individual is paying for the full cost of the treatment out-of-pocket.

These new requirements, when they become effective, may necessitate changes to HIPAA privacy notices and may also require amendments to the HIPAA-related provisions in group health plan documents and summary plan descriptions.

### ***Business Associates***

***Breach Notification.*** Notify the covered entity whenever “unsecured” PHI is breached. Such notification should be made without unreasonable delay and in any event within 60 days of discovery (or within 60 days of the date the breach should have been discovered). The notice must identify each individual whose unsecured PHI is breached. It should also contain the information necessary for the covered entity to satisfy its notification obligations with respect to each affected individual.

Business associates are already required to report to covered entities security breaches under the terms of current business associate agreements. However, new regulations regarding the security breach notification requirements will be issued by August 16, 2009, and compliance with those rules will be required 30 days after the regulations are published.

***Accounting for Disclosures.*** Provide an individual upon request with an accounting of disclosures of the information in her EHR over the last three years, including disclosures made for the purpose of treatment, payment or health care operations. In satisfying its obligation to provide an accounting of disclosures, a covered entity can elect to provide either an accounting of all disclosures made by it and each of its business associates, or an accounting of all disclosures made by it and the contact information for each of its business associates. If the latter approach is taken by the covered entity, then business associates will be required to respond directly to a requesting individual with an accounting. Covered entities and business associates may want to negotiate, as part of the business associate agreement, which of these two options the covered entity will utilize.

- For business associates who acquired an EHR after January 1, 2009, this requirement will apply to disclosures from such record made on or after January 1, 2011.
- For business associates who acquired an EHR on or before January 1, 2009, this requirement will apply to disclosures from such a record made on or after January 1, 2014.

***Prohibition on Sale of PHI.*** Follow the same rules prohibiting sale of PHI that apply to covered entities. Note that these rules do not preclude a business associate from being paid for services performed on behalf of a covered entity.

***Restrictions on Marketing.*** Follow the same rules restricting marketing that apply to covered entities.

***Satisfaction of “Minimum Necessary.”*** Follow the same rules regarding use of limited data sets that apply to covered entities.

***HIPAA Security Rules.*** Starting on February 17, 2010, follow the HIPAA security rules previously applicable only to covered entities. Business associates will be required to appoint a security officer; develop written security policies and procedures; adopt administrative, physical and technical safeguards for PHI; and train its workforce on how to protect PHI. HHS is required to issue guidance on appropriate technical safeguards for PHI.



*Terminate Contract/Notify HHS If Covered Entity Violates HIPAA.* If a business associate becomes aware that the covered entity with whom it has contracted has engaged in a pattern or practice that constitutes a material violation of certain of HIPAA’s requirements, and if the covered entity does not take steps to cure the violation, then the business associate must terminate the contract or, if termination is not feasible, report the violation to HHS.

***Further Explanation of Business Associate Changes***

*Pre-ARRA.* Before ARRA, business associates were not directly regulated by HIPAA or subject to HIPAA’s penalties. They did have a contractual obligation to follow certain HIPAA privacy and security rules, which were required by law to be in their business associate agreements, but negative consequences rarely followed a breach (occurring only if the covered entity sustained economic damages and sued the business associate for failing to live up to its contract).

*Post-ARRA.* With the passage of ARRA, effective February 17, 2010, the HIPAA *security* rules will apply directly to business associates for the first time. The HIPAA *privacy* rules will still, for the most part, apply only through operation of the business associate agreement. However, a breach of the privacy requirements contained in a business associate agreement will now be punishable under HIPAA.

*Effect on Business Associate Agreements.* Existing business associate agreements will have to be revised to reflect the new requirements described above. Depending on the terms of existing business associate agreements and the desire of the parties to document each of their respective legal obligations, revisions may be necessary when the new breach notification requirements become effective which, at the latest, will be September 15, 2009.

*New Entities Subject to Same Requirements as Business Associates.* ARRA also subjects additional entities to certain of the requirements applicable to business associates. Entities that provide data transmission of PHI to covered entities or their business associates, such as health information exchange organizations and vendors of personal health records (PHR), must enter into a written agreement with the covered entity containing the same requirements applicable to business associates.

**INCREASED PENALTIES**

Besides extending the penalties for HIPAA security and privacy violations to business associates effective February 17, 2010, ARRA has increased the amount of civil penalties currently applicable to covered entities, effective immediately. HIPAA had set the *maximum* civil penalty for security and privacy violations at \$100 per violation (and at \$25,000 for the total amount imposed on a person for all such violations of an identical requirement for a calendar year). Under ARRA, the \$100 figure above is now a *minimum* instead of a maximum, and higher minimum penalties apply based on the facts and circumstances of the violation.

Criteria for Determining Penalty	Minimum Penalty (Per Violation/Cap)	Maximum Penalty (Per Violation/Cap)
Violator did not know and could not have been expected to know about the violation	\$100/\$25,000	\$50,000/\$1,500,000
There was “reasonable cause” and no “willful neglect”	\$1,000/\$100,000	\$50,000/\$1,500,000
There was willful neglect and violation was corrected	\$10,000/\$250,000	\$50,000/\$1,500,000
There was willful neglect and violation was not corrected	\$50,000/\$1,500,000	No specified maximum



## IMPROVED ENFORCEMENT

**Enforcement by State Attorneys General.** Effective immediately, state attorneys general are authorized to bring civil actions against violators in federal district court.

**Audits by HHS.** ARRA mandates that HHS conduct periodic audits to ensure that covered entities are in compliance with HIPAA privacy and security requirements.

**Mandatory Investigations and Penalties.** HHS is required to conduct a formal investigation if a preliminary investigation of the facts of a complaint indicates willful neglect. It is also required to impose penalties anytime a HIPAA violation is accompanied by willful neglect. These enforcement mechanisms will become effective upon the issuance of regulations no later than August 18, 2010.

**Distribution of Penalties Collected.** HHS is required to establish a process within the next three years whereby individuals affected by a HIPAA violation may receive a percentage of any penalty or settlement collected with respect to that violation. Note that this enforcement mechanism in particular will provide a powerful financial incentive to plaintiffs and plaintiffs' counsel to monitor covered entities and business associates closely for HIPAA violations.

## NON-STATUTORY DEVELOPMENTS RELATED TO HIPAA SECURITY

**CVS Caremark Settlement.** An example of what may be in store for covered entities and business associates under a stronger enforcement regime can be gleaned from the recent news report involving CVS Caremark. CVS became the subject of a federal investigation in 2006 when media reported that its paper records were being tossed into publicly accessible dumpsters. Just one month before ARRA was signed into law, CVS entered into an agreement with HHS and the FTC settling the data privacy and security allegations to the tune of \$2.25 million.

**HHS Q&As Regarding Disposal of PHI.** On February 18, 2009, HHS posted on its web site answers to questions that the settlement likely elicited. These Q&As provide the following clarifications regarding the proper disposal of PHI:

- PHI may not be disposed of in dumpsters that are accessible by unauthorized persons unless the information has first been rendered permanently indecipherable;
- A covered entity who hires a business associate to dispose of PHI must enter into a written agreement requiring that the disposal be conducted in a secure manner;
- When reusing or disposing of computers, covered entities must take steps to remove PHI; and
- Workers who use PHI off-site must receive training on and follow appropriate disposal policies and procedures.

## RECOMMENDED ACTION ITEMS

Because increased penalties for non-compliance are effective immediately, it is recommended that covered entities, including sponsors of group health plans, review and refresh their compliance efforts with respect to pre-ARRA HIPAA requirements and the newly posted guidance regarding disposal of PHI. Some questions to consider:

- Are your HIPAA privacy and security officer designations up-to-date?
- Have you recently reviewed your privacy and security practices and procedures to ensure that they are still in place, and have you documented any changes or improvements to such procedures? Note that as



you review existing policies and procedures, be sure to specifically review procedures for the disposal of PHI, and compare them to the guidance recently posted by HHS.

- Have you conducted HIPAA training or refresher training for employees who handle PHI?
- Have you confirmed that business associate agreements are in place with all current business associates? As you check the status of these agreements, keep them handy, as modifications to these agreements will be necessary once applicable guidance has been issued.
- Have you reviewed your privacy policy recently, and are you in compliance with the requirements for providing a copy of the policy to health plan participants every three years?

Business associates should be conducting this same type of exercise and will likely have to enhance their privacy and security policies and procedures, employee training efforts, etc. to prepare for the increased security requirements and penalties for non-compliance that will take effect in 12 months.

Both covered entities and business associates should also begin taking steps in preparation for compliance with the breach notification rules and the EHR accounting rules.

#### **FOR MORE INFORMATION**

The members of Thompson Hine's Employee Benefits & Executive Compensation practice group and our Privacy and Information Security Team stand ready to assist you with:

- HIPAA compliance reviews
- Drafting and negotiating business associate agreements
- Employee training
- Data breach notifications
- Notification and explanation of future guidance

If you would like more information, please contact your primary Thompson Hine lawyer or email us at [AskUs@ThompsonHine.com](mailto:AskUs@ThompsonHine.com).

Thompson Hine sends bulletins as a service. If you do not wish to receive future bulletins, please email [Heidi.Moreno@ThompsonHine.com](mailto:Heidi.Moreno@ThompsonHine.com) with the phrase "Unsubscribe" as the subject line.

This advisory may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgement of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions. Some of the design images and photographs in this document may be of actors depicting fictional scenes.

© 2009 THOMPSON HINE LLP. ALL RIGHTS RESERVED.