



Privacy and Security Provisions in the American Recovery and Reinvestment Act of 2009

The American Recovery and Reinvestment Act of 2009 (ARRA), also known as the “economic stimulus” bill, was signed by President Obama on Feb. 17, 2009. Title XIII of Division A of ARRA is called the Health Information Technology for Economic and Clinical Health (HITECH) Act.

The HITECH Act contains financial incentives, grants and loans to assist hospitals in adopting electronic health record (EHR) systems, penalties in the future for hospitals that fail to adopt EHRs, and, in Subtitle D, privacy and security enhancements. This document outlines the privacy and security provisions in the HITECH Act, and the many guidances and regulations required to be published over the next three years.

This memo summarizes the HITECH Act. It does not include related provisions of California law.

DEFINITIONS

Section 13400 (42 U.S.C. Sec. 17921)

This section contains definitions of many terms, most of which are already defined in the HIPAA regulations. Only the new terms and their definitions are included in this summary.

The term “**breach**” means the unauthorized acquisition, access, use, or disclosure of Protected Health Information (PHI) that compromises the security or privacy of the PHI, unless the recipient would not reasonably have been able to retain the information.

Exceptions — the term “breach” does not include:

1. Unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of a Covered Entity (CE) or Business Associate (BA) if:
 - a. The acquisition, access, or use was made in good faith and within the course and scope of employment (or other professional relationship); and
 - b. The PHI is not further acquired, accessed, used, or disclosed by any person; or
2. Inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility to another similarly situated individual at the same facility; and
3. The PHI is not further acquired, accessed, used, or disclosed without authorization.

The term “**electronic health record**” means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

The term “**personal health record**” means an electronic record of patient identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

The term “**vendor of personal health records**” means an entity, other than a covered entity, that offers or maintains a personal health record.

APPLICATION OF SECURITY PROVISIONS TO BUSINESS ASSOCIATES

Section 13401 (42 U.S.C. Sec. 17931)
(Effective Feb. 18, 2010)

This section states that the HIPAA and HITECH security provisions apply to BAs in the same manner that they apply to covered entities. These security provisions must be incorporated into the Business Associate Agreement (BAA).

If a BA violates a security provision, the BA is subject to HIPAA’s civil and criminal penalties.

REGULATIONS: Regulations are not required by the HITECH Act, but the Secretary plans to issue regulations to extend certain HIPAA Security Rule provisions to BAs by Feb. 18, 2010.

GUIDANCE: The Secretary must annually issue guidance on the most effective and appropriate technical safeguards. The first update is expected Feb. 18, 2010.

BREACH NOTIFICATION

Section 13402 (42 U.S.C. Sec. 17932)
(Effective for breaches discovered 30 days after publication of interim final regulations which are due by Aug. 18, 2009)

A CE that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured PHI must notify each individual whose unsecured PHI has been, or is reasonably believed by the CE to have been, accessed, acquired, or disclosed as a result of the breach.

REGULATIONS: The Secretary must issue interim final regulations regarding breach notification by Aug. 18, 2009. The provisions of this section are effective for breaches discovered 30 days after publication of the interim final regulations.

“**Unsecured PHI**” means PHI that is not secured through the use of a technology or methodology specified by the Secretary in guidance. The Secretary published the required guidance in the *Federal Register* on April 27, 2009. In it, the Secretary identified two methods of rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals:

1. Encryption:

- a. For data at rest, covered entities should refer to NIST Special Publication 800-111.
- b. For data in motion, covered entities should refer to FIPS 140-2.

2. Destruction:

- a. Paper, film, or other hard copy media must be shredded or destroyed such that PHI cannot be read or reconstructed.
- b. Electronic media must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88 such that media cannot be retrieved.

NOTE: Covered entities are not required to follow the guidance. However, if the specified technologies and methodologies are used, no breach notification obligation exists even if a breach occurs (“safe harbor”).

GUIDANCE: The Secretary must annually update this guidance. In addition, the guidance may be updated before the breach notification requirement becomes effective.

A BA that discovers a breach must notify the CE. The notice must include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed.

Timeline

Notification of the breach must be made without unreasonable delay and in no case later than 60 calendar days after discovery.

However, if a law enforcement official determines that a notification, notice, or web posting would impede a criminal investigation or cause damage to national security, the notification, notice or posting must be delayed for the time specified by the law enforcement official, if the official provides the CE with a written statement that notification would be reasonably likely to impede law enforcement activities and specifying the time for which notification should be delayed. If the law enforcement statement is made orally, the CE must:

1. Document the statement, including the identity of the law enforcement agency or official making the statement;
2. Temporarily refrain from notifying the individual of the breach; and
3. Limit the delay in notification to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time. [See 45 C.F.R. Section 164.528(a)(2)].

A breach is treated as discovered when any employee, officer, or other agent of the CE or BA, other than the individual committing the breach, knew, or should reasonably have known, about the breach.

The CE or BA has the burden of demonstrating that all notifications were made, including evidence demonstrating the necessity of any delay.

Method of Notice

Notification should be made by first-class mail at the last known address, unless the individual specifies a preference for e-mail. Notification may be provided in one or more mailings as information is available. If the individual is deceased, next of kin must be notified.

If there is insufficient or out-of-date contact information that precludes direct written notification, a substitute form of notice must be provided. If there are 10 or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting on the home page of the CE's website (for a period of time determined by the Secretary) or notice in major print or broadcast media (including major media in geographic areas where the individuals affected by the breach likely reside) is required. The web posting or media notice must include a toll-free phone number an individual can call to learn whether his or her unsecured PHI was included in the breach.

If the CE believes it is urgent to notify individuals of the breach because of possible imminent misuse of unsecured PHI, the CE may notify individuals by phone or other means as appropriate. However, a written notification must also be made.

Required Media Notice

If there is a breach of unsecured PHI of more than 500 residents of a state or jurisdiction, notice must be provided to prominent media outlets serving that state or jurisdiction. (There is no definition of the word "jurisdiction.")

Notice to the Department of Health and Human Services (DHHS)

A CE must notify the Secretary of DHHS of unsecured PHI that was acquired or disclosed in a breach. If the breach affected 500 or more individuals, the notice must be provided immediately. If the breach affected fewer than 500 individuals, the CE may maintain a log and annually submit the log.

DHHS will maintain a website identifying each CE involved in a breach in which the unsecured PHI of more than 500 individuals is acquired or disclosed. In addition, DHHS is required to submit a report to Congress regarding breaches by Feb. 18, 2010 and annually thereafter.

Content of Notice

Regardless of the method of notice provided to individuals, notice must include, to the extent possible, the following:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of unsecured PHI that were involved in the breach, such as full name, Social Security number, date of birth, home address, account number, or disability code.

3. The steps individuals should take to protect themselves from potential harm resulting from the breach.
4. A brief description of what the CE is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.
5. Contact procedures for individuals to ask questions, which must include a toll-free telephone number, an e-mail address, website, or postal address.

PRIVACY EDUCATION

Section 13403 (42 U.S.C. Sec. 17933)

By Aug. 18, 2009, the Secretary of DHHS must designate an individual in each regional office to offer guidance and education to CEs, BAs, and individuals on their rights and responsibilities related to federal privacy and security requirements.

By Feb. 18, 2010, the DHHS Office for Civil Rights must develop and maintain a “multi-faceted national education initiative to enhance public transparency regarding the uses of” PHI. This will include educating individuals about the potential uses of their PHI, the effects of such uses, and the rights of individuals with respect to such uses.

APPLICATION OF PRIVACY PROVISIONS TO BUSINESS ASSOCIATES

Section 13404 (42 U.S.C. Sec. 17934)

(Effective Feb. 18, 2010)

A BA may use and disclose PHI only if such use or disclosure complies with the BA contract and the HIPAA BA contract requirements. The privacy provisions in the HITECH Act apply to BAs and must be incorporated into BAAs.

If a BA learns of a pattern or practice of a CE that constitutes a material breach of privacy or security requirements, the BA must terminate the contract if feasible, or notify the Secretary if termination is not feasible, unless the CE cures the breach or ends the violation.

If a BA violates a privacy provision, the BA is subject to HIPAA’s civil and criminal penalties.

REGULATIONS: Regulations are not required by the HITECH Act, but the Secretary plans to issue regulations to extend certain HIPAA Privacy Rule provisions to BAs by Feb. 18, 2010.

NEW RESTRICTIONS AND REQUIREMENTS

Section 13405 (42 U.S.C. Sec. 17935)

Requested Restrictions on Certain Disclosures of Health Information

(Effective Feb. 18, 2010)

If an individual requests a restriction on disclosure of PHI to a health plan, the provider *must* comply with the requested restriction, if the disclosure is for purposes of carrying out payment or

health care operations, and the PHI pertains *solely* to an item or service for which the provider has been paid out of pocket in full.

NOTE: This provision still permits disclosure of the PHI to the health plan for *treatment* purposes, or other purposes not including payment or health care operations. However, hospitals should exercise caution in disclosing information for treatment or other permitted purposes when the individual has requested no information be disclosed for purposes of payment and health care operations. Hospitals should develop policies and procedures that cover such situations.

REGULATIONS: Regulations are not required by the HITECH Act, but the Secretary plans to issue regulations to modify the HIPAA Privacy Rule's provision regarding the right to request restrictions by Feb. 18, 2010.

Disclosures Required to be Limited to the Limited Data Set or the Minimum Necessary
(Effective Feb. 18, 2010)

A CE shall be treated as being in compliance with the “minimum necessary” standard with respect to the use, disclosure, or request of PHI only if the CE limits the PHI *to the extent practicable* to the limited data set or, if needed, to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The CE or BA disclosing the PHI is the entity that determines what constitutes the minimum necessary to accomplish the intended purpose of the disclosure — not the person requesting the PHI.

This requirement shall not apply after the effective date on which the Secretary issues the guidance noted below. This requirement shall not be construed as affecting the use, disclosure, or request of PHI that has been de-identified.

GUIDANCE: By Aug. 18, 2010, the Secretary is required to issue guidance on what constitutes “minimum necessary” for purposes of the HIPAA privacy regulations. In issuing this guidance, the Secretary must consider the guidance required under Section 13424(c) regarding how best to implement the requirements for de-identification of PHI (due Feb. 18, 2010) and the information necessary to improve patient outcomes and to detect, prevent, and manage chronic disease.

REGULATIONS: Regulations are not required by the HITECH Act, but the Secretary plans to issue regulations to modify the HIPAA Privacy Rule's provision regarding “minimum necessary” by Feb. 18, 2010.

Accounting of Certain PHI Disclosures Required if CE Uses EHR
(Effective date depends upon when CE acquires EHR. See below.)

A CE must provide an accounting of disclosures through an EHR for treatment, payment or health care operations purposes for 3 years prior to the date on which the accounting is requested.

REGULATIONS: The Secretary shall promulgate regulations on what information must be collected about each disclosure for treatment, payment, and health care operations purposes through an EHR, not later than 6 months after the date on which the Secretary adopts standards on accounting for disclosure described in Section 13101 of the HITECH Act (Section 3002(b)(2)(B)(iv) of the Public Health Service Act) which requires the HIT Policy Committee to recommend technologies that as part of a qualified EHR allow for an accounting of disclosures for TPO. The regulations are expected by June 18, 2010.

If an individual requests an accounting, the CE must provide either an accounting of disclosures by the CE and all of its BAs, or an accounting of disclosures by the CE and a list of all BAs. The list of BAs must include contact information for each BA, such as mailing address, phone, and e-mail address. BAs must provide an accounting of disclosures upon request of an individual.

For CEs that acquired an EHR on or before Jan. 1, 2009, the effective date of this requirement is Jan. 1, 2014. For CEs that acquired an EHR after Jan. 1, 2009, the effective date is the later of Jan. 1, 2011 or the date the CE acquires the EHR. The Secretary of DHHS may delay effective dates by up to 2 years.

Prohibition on Sale of EHR or PHI

(Effective for exchanges occurring on or after the date that is 6 months after the promulgation of final regulations noted below.)

A CE or BA may not, directly or indirectly, receive remuneration in exchange for any PHI without the individual's HIPAA-compliant authorization. The authorization form must state whether the PHI can be further exchanged for remuneration by the entity receiving the PHI. The following are exceptions to this general rule:

1. The purpose of the exchange is for public health activities.
2. The purpose of the exchange is for research, and the price charged reflects the costs of preparation and transmittal of the data.
3. The purpose of the exchange is for the treatment of the individual.
4. The purpose of the exchange is the sale, transfer, merger, or consolidation of all or part of the CE, and due diligence related to such activity [see 45 C.F.R. Section 164.501(6)(iv)];
5. The purpose of the exchange is for remuneration provided by a CE to a BA for activities involving the exchange of PHI that the BA undertakes on behalf of, and at the specific request of, the CE pursuant to a BAA.
6. The purpose of the exchange is to provide an individual with a copy of his or her PHI.
7. Another exception promulgated by the Secretary in regulations. At this time, there are no other exceptions.

REGULATIONS: By Aug. 18, 2010, the Secretary shall promulgate regulations to carry out these limitations regarding the sale of EHR and PHI.

Access to Certain Information in Electronic Format

(Effective Feb. 18, 2010)

If a CE maintains an EHR, the individual may choose to receive the PHI that he/she has a right to access in an electronic format. In addition, the patient may direct the CE to transmit an electronic copy directly to another entity or person, provided that the choice is clear, conspicuous, and specific. The CE may charge the individual the usual fees as permitted by HIPAA, but the charge must be capped at the amount equal to the labor costs in responding to the request for the copy (or summary or explanation).

REGULATIONS: Regulations are not required by the HITECH Act, but the Secretary plans to issue regulations to modify the HIPAA Privacy Rule's provision regarding electronic access by Feb. 18, 2010.

CONDITIONS ON CERTAIN CONTACTS AS PART OF HEALTH CARE OPERATIONS

Section 13406 (42 U.S.C. Sec. 17936)

(Effective for written communications occurring on or after Feb. 18, 2010)

Marketing

The HITECH Act limits the scope of marketing that is considered "health care operations." This means that some marketing activities that are currently considered "health care operations" will in the future require a HIPAA-compliant patient authorization.

For providers, "**marketing**" is currently defined as:

1. Making a communication about a product or service that encourages recipients to purchase or use the product or service, *unless* that communication is made:
 - a. To describe a health-related product or service that is provided by the CE making the communication;
 - b. For treatment of the individual; or
 - c. For case management or care coordination, to direct or recommend alternative treatments, providers, or settings of care.
2. An arrangement between a CE and any other entity whereby the CE discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients to purchase or use it.

Effective for written communications occurring on or after Feb. 18, 2010, the arrangement described in item 2 above is not considered a health care operation. Thus, a CE will need a HIPAA-compliant authorization to make such disclosures.

In addition, effective for written communications occurring on or after Feb. 18, 2010, the communications described in item 1 above will not be considered health care operations if the CE receives direct or indirect payment in exchange for making the communication, except where:

1. The communication describes only a drug or biologic that is currently prescribed for the recipient of the communication; and any payment received by the CE is reasonable in amount; or
2. The communication is made by the CE and the CE obtains a HIPAA-compliant authorization, or the communication is made by a BA on behalf of a CE and the communication is consistent with the BAA

REGULATIONS: The Secretary shall promulgate regulations to define the term “reasonable amount.” There is no deadline for these regulations, but the Secretary plans to issue them by Feb. 18, 2010.

The term “direct or indirect payment” does not include payment for the treatment provided to the patient.

Fundraising

Any fundraising communication must, in a clear and conspicuous manner, provide an opportunity for the recipient to elect not to receive further fundraising communications.

REGULATIONS: The Secretary shall promulgate regulations to implement the fundraising “opt out” requirement. There is no deadline for these regulations, but the Secretary plans to issue them by Feb. 18, 2010.

CLARIFICATION OF APPLICATION OF WRONGFUL DISCLOSURES/CRIMINAL PENALTIES

*Section 13409 (amends 42 U.S.C. Sec. 1320d-6(a))
(Effective Feb. 18, 2010)*

The HITECH Act adds one sentence to the end of the existing statute establishing criminal penalties for HIPAA violations. The new sentence states that, for purpose of imposing criminal penalties, “a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity ... and the individual obtained or disclosed such information without authorization.”

This language clarifies that employees and other individuals, in addition to covered entities, may be subject to criminal penalties for HIPAA violations. This clarification was in response to a DHHS/DOJ legal opinion that only covered entities could be held criminally liable — not the employees of covered entities.

IMPROVED ENFORCEMENT

Section 13410 (42 U.S.C. Sec. 17939; amends 42 U.S.C. Sec. 1320d-5)

Any violation of the HITECH Act privacy or security provisions is subject to HIPAA penalties.

REGULATIONS: Regulations are not required, but the Secretary plans to issue regulations to revise the HIPAA Enforcement Rule by Feb. 18, 2010.

Noncompliance Due to Willful Neglect

The Secretary of DHHS is required to formally investigate any complaint if a preliminary investigation of the facts indicates a possible violation due to willful neglect. The Secretary must impose a financial penalty under the civil penalties law [42 U.S.C. Sec. 1320d-5(a)(1)] if it finds a violation due to willful neglect.

REGULATIONS: By Aug. 18, 2010, the Secretary shall promulgate regulations to implement the provisions related to noncompliance due to willful neglect. These provisions will apply to penalties imposed on or after Feb. 18, 2011.

Distribution of Civil Monetary Penalties Collected

(Effective Feb. 18, 2010)

Any civil monetary penalty or settlement collected for a violation of HIPAA or the HITECH Act privacy or security requirements will be transferred to the Office for Civil Rights to be used for further enforcement.

Individuals who are harmed will be entitled to a percentage of any civil monetary penalty or settlement collected.

REPORT/REGULATIONS: By Aug. 18, 2010, the Comptroller General must submit to the Secretary of DHHS a report including recommendations for a methodology under which an individual who is harmed by a violation of HIPAA or the HITECH Act may receive a percentage of any civil monetary penalty or settlement collected. By Feb. 18, 2012, the Secretary must promulgate regulations establishing a methodology to give harmed individuals a part of any penalties collected. This methodology will be applied to penalties/settlements imposed on or after the effective date of the regulation.

Tiered Increase in Amount of Civil Monetary Penalties

(Effective for violations occurring after Feb. 18, 2009)

The HITECH Act revises the civil monetary penalty provision of HIPAA as follows:

1. Penalties where the **violation did not know (and by exercising reasonable diligence would not have known)**: from \$100 to \$50,000 per violation. (There is a cap for repeated violations of an *identical* requirement or prohibition during a calendar year of \$25,000 to \$1.5 million.)

2. Penalties where the **violation was due to reasonable cause and not to willful neglect**: from \$1,000 to \$50,000 per violation. (There is a cap for repeated violations of an *identical* requirement or prohibition during a calendar year of \$100,000 to \$1.5 million.)
3. Penalties where the **violation was due to willful neglect**: from \$10,000 to \$50,000 per violation, if the violation is corrected pursuant to 42 U.S.C. Section 1320d-5(b)(3)(A), which requires correction within 30 days of the date the person knew, or by exercising reasonable diligence, would have known, of the violation. (There is a cap for repeated violations of an *identical* requirement or prohibition during a calendar year of \$250,000 to \$1.5 million.)
4. Penalties where the **violation was due to willful neglect and not corrected**: \$50,000 per violation. (There is a cap for repeated violations of an *identical* requirement or prohibition during a calendar year of \$1.5 million.)

In determining the amount of a penalty, the Secretary must base its determination on the nature and extent of the violation and the nature and extent of the harm resulting from the violation.

Enforcement through State Attorneys General (Effective Feb. 18, 2009)

The HITECH Act permits state attorneys general to bring a civil action in U.S. District Court to enjoin further violations or to obtain monetary damages. The amount of monetary damages will be calculated by multiplying the number of violations by up to \$100. The total amount of damages imposed on a person for all violations *of an identical requirement or prohibition* during a calendar year may not exceed \$25,000. In assessing the damages, the court will reduce the amount of damages after considering the factors the Secretary may consider in determining the amount of a civil monetary penalty (that is, if the failure to comply is due to reasonable cause and not to willful neglect, the penalty may be waived completely or the amount may be reduced if excessive relative to the compliance failure involved.) The attorney general may also recover attorneys fees and costs from the defendant.

The attorney general must notify the Secretary of DHHS of any lawsuit. The Secretary has the right to intervene.

A state attorney general must comply with the existing statute of limitations, and may not bring a lawsuit during the pendency of any action brought by the Secretary against a defendant regarding the same alleged violations.

Allowing the Office of Civil Rights (OCR) to Use Corrective Action without Penalty

The HITECH Act shall not be construed to prevent the OCR from using, at its discretion, corrective action without a penalty where the person did not know (and by exercising reasonable diligence would not have known) of the violation involved.

AUDITS

Section 13411 (42 U.S.C. Sec. 17940)
(Effective Feb. 18, 2010)

The Secretary will provide for periodic audits of CEs and BAs for compliance with HIPAA privacy and security requirements.

RELATIONSHIP TO OTHER LAWS

Section 13421 (42 U.S.C. Sec. 17951)

The existing HIPAA preemption rules apply to the provisions in the HITECH Act.

STUDIES, REPORTS, GUIDANCE

Section 13424 (42 U.S.C. Sec. 17954)

By Feb. 18, 2010 and annually thereafter, the Secretary must submit a report to Congress regarding complaints of violations of HIPAA privacy and security requirements. The report will include the number of complaints, how they were resolved, penalties imposed, the number of compliance reviews and audits, and other similar information.

By Feb. 18, 2010, the Secretary must submit a report to Congress on privacy, security and breach notification requirements for entities that are not CEs or BAs, such as vendors of PHRs. The Secretary must also submit a recommendation of which federal government agency is best equipped to regulate these entities and a timeframe for implementing regulations.

By Feb. 18, 2010, the Secretary must issue guidance on how best to implement the requirements for de-identification of PHI.

By Feb. 18, 2010, the U.S. Comptroller General must submit a report to Congress on best practices related to the disclosure of PHI among health care providers for treatment purposes. The report will include, among other things, an examination of the use of electronic informed consent for disclosing PHI for treatment, payment, and health care operations purposes.

By Feb. 18, 2014, the Government Accountability Office must submit a report to Congress on the impact of any of the provisions of the HITECH Act on health insurance premiums, overall health care costs, adoption of EHRs by providers, and reduction in medical errors and other quality improvements.

The Secretary must study the definition of “psychotherapy notes” with regard to including test data that are a part of a mental health evaluation. The Secretary may (but isn’t required to) issue regulations to revise this definition. There is no deadline for this study, but it is expected by Feb. 18, 2010.

QUESTIONS

Questions about the HITECH Act, or privacy legal questions in general, may be directed to Lois Richardson, lrichardson@calhospital.org, (916) 552-7611.

LJR: acl