COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual 2024
Health Information Technology for Economic and Clinical Health Act

By Gabriel Imperato,[1] Esq., CHC; Anne Novick Branan,[2] Esq., CHC; Richard Sena[3] ; and Megan Speltz,[4] JD

Fast Facts

Title of law: Health Information Technology for Economic and Clinical Health (HITECH) Act

Categories:

- Medical records
- Privacy
- Cybersecurity
- Data protection

U.S. Code: 42 U.S.C. §§ 17937, 17953

Public law: Pub. L. No. 111-5, 123 Stat. 226

Year enacted: 2009

Major amendments: Not applicable.

Enforcement agency: U.S. Department of Health & Human Services' Office for Civil Rights (OCR)

Link to full text of law:
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentitie

Applies to: All health plans, healthcare clearinghouses, healthcare providers, and endorsed sponsors of the Medicare prescription drug discount card, including business associates that supply services and certain functions for covered entities and have access to personal health information.

What Is the Health Information Technology for Economic and Clinical Health Act?

The Health Information Technology for Economic and Clinical Health (HITECH) Act was created to motivate the implementation of electronic health records (EHRs) and supporting technology in the United States. The act

implemented changes such as:[5]

- Increasing Health Insurance Portability and Accountability Act (HIPAA) enforcement and penalties;
- Requiring notification to patients of any unsecured data breaches related to protected health information (PHI), and notifying the U.S. Department of Health & Human Services (HHS) if the breach affected more than 500 patients;
- Giving patients and designated third parties access to their PHI in an electronic format; and
- Extending HIPAA requirements to apply to business associates.

History

The HITECH Act was signed into law by President Barack Obama on February 17, 2009, as part of the American Recovery and Reinvestment Act of 2009 (ARRA), an economic stimulus bill.[6] It was passed to promote the expansion of health information technology (IT) and the adoption of EHRs by healthcare organizations by providing incentives for organizations to migrate from paper to electronic records. Prior to the HITECH Act's adoption, only 10% of hospitals had adopted EHRs.[7] Since the act's passage, the EHR adoption rate dramatically increased, and, as of 2017, 86% of office-based physicians have moved to EHRs. Accordingly, the HITECH Act has caused a significant growth in healthcare technology fields, such as research informatics, IT, electronic medical records, and other related disciplines.[8]

The HITECH Act is split into four subtitles, with each focusing on either promotion and funding of health IT or strengthening privacy, security, and enforcement of existing HIPAA rules.[9] The act strengthened HIPAA's Privacy and Security rules by increasing enforcement penalties and expanding HIPAA compliance to business associates of covered entities. Further, the act imposed a data breach notification requirement and increased the protection of electronic protected health information (ePHI). The HITECH Act also gave the HHS Office of the National Coordinator for Health Information Technology (ONC) the authority to manage and set standards for promoting and expanding the adoption of health information technology.

Related Laws

Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191

The HITECH Act bolsters the scope, language, and enforcement penalties of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA established national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. It consists of a number of rules that lay out different requirements for HIPAA compliance.

HIPAA was enacted to:[10]

- Improve portability and continuity of health insurance coverage;
- Combat waste, fraud, and abuse in health insurance and healthcare delivery;
- Promote the use of medical savings accounts; and
- Improve access to long-term care services and coverage to simplify the administration of health insurance.

For more information on this law, please see the "HIPAA" article in this chapter.

Health Information Technology for Economic and Clinical Health Act Compliance Risks

Risk Area: Individuals' Right to Access PHI in Electronic Format

> e. Access to certain information in electronic format
>
> In applying section 164.524 of title 45, Code of Federal Regulations, in the case that a covered entity uses or maintains an electronic health record with respect to protected health information of an individual—
>
> 1. the individual shall have a right to obtain from such covered entity a copy of such information in an electronic format and, if the individual chooses, to direct the covered entity to transmit such copy directly to an entity or person designated by the individual, provided that any such choice is clear, conspicuous, and specific;
>
> 2. if the individual makes a request to a business associate for access to, or a copy of, protected health information about the individual, or if an individual makes a request to a business associate to grant such access to, or transmit such copy directly to, a person or entity designated by the individual, a business associate may provide the individual with such access or copy, which may be in an electronic form, or grant or transmit such access or copy to such person or entity designated by the individual; and
>
> 3. notwithstanding paragraph (c)(4) of such section, any fee that the covered entity may impose for providing such individual with a copy of such information (or a summary or explanation of such information) if such copy (or summary or explanation) is in an electronic form shall not be greater than the entity's labor costs in responding to the request for the copy (or summary or explanation).[11]

Context: Considering the HITECH Act's promotion of ePHI, the act also imposed a requirement that such information may be transmitted in electronic format to an individual upon request. This includes a request made by an individual to transmit ePHI to another entity. Considering the complexity in providing ePHI while maintaining security and privacy standards, healthcare organizations are permitted to charge a fee commensurate with the cost of transmitting the ePHI.

Risk Area: Application of HIPAA Security and Privacy Rules on Business Associates

> a. Application of contract requirements
>
> In the case of a business associate of a covered entity that obtains or creates protected health information pursuant to a written contract (or other written arrangement) described in section 164.502(e)(2) of title 45, Code of Federal Regulations, with such covered entity, the business associate may use and disclose such protected health information only if such use or disclosure, respectively, is in compliance with each applicable requirement

of section 164.504(e) of such title. The additional requirements of this subchapter that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.

b. Application of knowledge elements associated with contracts

Section 164.504(e)(1)(ii) of title 45, Code of Federal Regulations, shall apply to a business associate described in subsection (a), with respect to compliance with such subsection, in the same manner that such section applies to a covered entity, with respect to compliance with the standards in sections 164.502(e) and 164.504(e) of such title, except that in applying such section 164.504(e)(1)(ii) each reference to the business associate, with respect to a contract, shall be treated as a reference to the covered entity involved in such contract.

c. Application of civil and criminal penalties

In the case of a business associate that violates any provision of subsection (a) or (b), the provisions of sections 1176 and 1177 of the Social Security Act (42 U.S.C. §§ 1320d–5, 1320d–6) shall apply to the business associate with respect to such violation in the same manner as such provisions apply to a person who violates a provision of part C of title XI of such Act [42 U.S.C. § 1320d et seq.].[12]

Context: Various nonhealthcare provider or insurance provider organizations that have access to PHI were not subject to HIPAA's Privacy and Security rules prior to the HITECH Act's passage. The HITECH Act stretched HIPAA's umbrella over business associates, which include entities such as claims processors, accountants, law firms, consultants, or any other entity that routinely handles PHI to service a healthcare provider or another business associate.[13]

Risk Area: Required Notification of Breach

a. In general

A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, 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.

b. Notification of covered entity by business associate

A business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses

unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach.

c. Breaches treated as discovered

For purposes of this section, a breach shall be treated as discovered by a covered entity or by a business associate as of the first day on which such breach is known to such entity or associate, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such entity or associate, respectively) or should reasonably have been known to such entity or associate (or person) to have occurred.

d. Timeliness of notification

1. In general

Subject to subsection (g), all notifications required under this section shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by the covered entity involved (or business associate involved in the case of a notification required under subsection (b)).

2. Burden of proof

The covered entity involved (or business associate involved in the case of a notification required under subsection (b)), shall have the burden of demonstrating that all notifications were made as required under this part, including evidence demonstrating the necessity of any delay.

e. Methods of notice

1. Individual notice

Notice required under this section to be provided to an individual, with respect to a breach, shall be provided promptly and in the following form:

A. Written notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or, if specified as a preference by the individual, by electronic mail. The notification may be provided in one or more mailings as information is available.

B. In the case in which there is insufficient, or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes direct written (or, if specified by the individual under subparagraph (A), electronic) notification to the individual, a substitute form of notice shall be provided, including, in the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting for a period determined by the Secretary on the home page of the Web site of the covered entity involved or notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting will include a toll-free phone number where an individual can learn whether or not the individual's unsecured protected health information is possibly included in the breach.

C. In any case deemed by the covered entity involved to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity, in addition to notice provided under subparagraph (A), may provide information to individuals by telephone or other means, as appropriate.

2. Media notice

   Notice shall be provided to prominent media outlets serving a State or jurisdiction, following the discovery of a breach described in subsection (a), if the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

3. Notice to Secretary

   Notice shall be provided to the Secretary by covered entities of unsecured protected health information that has been acquired or disclosed in a breach. If the breach was with respect to 500 or more individuals than such notice must be provided immediately. If the breach was with respect to less than 500 individuals, the covered entity may maintain a log of any such breach occurring and annually submit such a log to the Secretary documenting such breaches occurring during the year involved.

4. Posting on HHS public website

   The Secretary shall make available to the public on the Internet website of the Department of Health and Human Services a list that identifies each covered entity involved in a breach described in subsection (a) in which the unsecured protected health information of more than 500

individuals is acquired or disclosed.

f. Content of notification

Regardless of the method by which notice is provided to individuals under this section, notice of a breach shall 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 protected health information 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 covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.

5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

g. Delay of notification authorized for law enforcement purposes

If a law enforcement official determines that a notification, notice, or posting required under this section would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed in the same manner as provided under section 164.528(a)(2) of title 45, Code of Federal Regulations, in the case of a disclosure covered under such section.

h. Unsecured protected health information

1. Definition

A. In general

Subject to subparagraph (B), for purposes of this section, the term "unsecured protected health information" means protected health information that is not secured through the use of a technology or methodology specified by the Secretary in the guidance issued under paragraph (2).

B. Exception in case timely guidance not issued

In the case that the Secretary does not issue guidance under paragraph (2) by the date specified in such paragraph, for purposes of this section, the term "unsecured protected health information" shall mean protected health information that is not secured by a technology standard that renders protected health information 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.

2. Guidance

For purposes of paragraph (1) and section 17937(f)(3) of this title, not later than the date that is 60 days after February 17, 2009, the Secretary shall, after consultation with stakeholders, issue (and annually update) guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals, including the use of standards developed under section 300jj–12(b)(2)(B)(vi) of this title, as added by section 13101 of this Act.

i. Report to Congress on breaches

1. In general

Not later than 12 months after February 17, 2009, and annually thereafter, the Secretary shall prepare and submit to the Committee on Finance and the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Ways and Means and the Committee on Energy and Commerce of the House of Representatives a report containing the information described in paragraph (2) regarding breaches for which notice was provided to the Secretary under subsection (e)(3).

2. Information

The information described in this paragraph regarding breaches specified in paragraph (1) shall include—

A. the number and nature of such breaches; and

B. actions taken in response to such breaches.

j. Regulations; effective date

To carry out this section, the Secretary of Health and Human Services shall promulgate interim final regulations by not later than the date that is 180 days after February 17, 2009. The provisions of this section shall apply to breaches that are discovered on or after the date that is 30 days after the

date of publication of such interim final regulations.[14]

Context: Breach notification is an important aspect of HIPAA imposed by the HITECH Act, prompting covered entities and business associates to self-report breaches of PHI. The Breach Notification Rule, which is codified under HIPAA at 45 C.F.R. §§ 164.404, 164.406, and 164.408 , requires that covered entities and business associates report breaches to individuals. If the breach exceeds 500 individuals, then the covered entity or business associate must notify the Secretary of the U.S. Department of Health & Human Services. If the breach exceeds 500 individuals in a particular state or jurisdiction, then the covered entity or business associate must notify local media outlets in that location of the breach.

Risk Area: Tougher Enforcement Penalties Under HIPAA

a. General penalty

1. In general

Except as provided in subsection (b), the Secretary shall impose on any person who violates a provision of this part—

A. in the case of a violation of such provision in which it is established that the person did not know (and by exercising reasonable diligence would not have known) that such person violated such provision, a penalty for each such violation of an amount that is at least the amount described in paragraph (3)(A) but not to exceed the amount described in paragraph (3)(D);

B. in the case of a violation of such provision in which it is established that the violation was due to reasonable cause and not to willful neglect, a penalty for each such violation of an amount that is at least the amount described in paragraph (3)(B) but not to exceed the amount described in paragraph (3)(D); and

C. in the case of a violation of such provision in which it is established that the violation was due to willful neglect—

i. if the violation is corrected as described in subsection (b)(3)(A),[1] a penalty in an amount that is at least the amount described in paragraph (3)(C) but not to exceed the amount described in paragraph (3)(D); and

ii. if the violation is not corrected as described in such subsection, a penalty in an amount that is at least the amount described in paragraph (3)(D).

In determining the amount of a penalty under this section for a violation, the Secretary shall base such determination on the nature and extent of the violation and the nature and extent of the harm resulting from such violation.

2. Procedures

   The provisions of section 1320a–7a of this title (other than subsections (a) and (b) and the second sentence of subsection (f)) shall apply to the imposition of a civil money penalty under this subsection in the same manner as such provisions apply to the imposition of a penalty under such section 1320a–7a of this title.

3. Tiers of penalties described

   For purposes of paragraph (1), with respect to a violation by a person of a provision of this part—

   A. the amount described in this subparagraph is $100 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $25,000;

   B. the amount described in this subparagraph is $1,000 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $100,000;

   C. the amount described in this subparagraph is $10,000 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $250,000; and

   D. the amount described in this subparagraph is $50,000 for each such violation, except that the total amount imposed on the person for all such violations of an identical requirement or prohibition during a calendar year may not exceed $1,500,000.

b. Limitations

1. Offenses otherwise punishable

   No penalty may be imposed under subsection (a) and no damages obtained under subsection (d) with respect to an act if a penalty has been imposed under section 1320d–6 of this title with respect to such act.

2. Failures due to reasonable cause

   A. In general

      Except as provided in subparagraph (B) or subsection (a)(1)(C), no penalty may be imposed under subsection (a) and no damages obtained under subsection (d) if the failure to comply is corrected

during the 30-day period beginning on the first date the person liable for the penalty or damages knew, or by exercising reasonable diligence would have known, that the failure to comply occurred.

B. Extension of period

i. No penalty

With respect to the imposition of a penalty by the Secretary under subsection (a), the period referred to in subparagraph (A) may be extended as determined appropriate by the Secretary based on the nature and extent of the failure to comply.

ii. Assistance

If the Secretary determines that a person failed to comply because the person was unable to comply, the Secretary may provide technical assistance to the person during the period described in subparagraph (A). Such assistance shall be provided in any manner determined appropriate by the Secretary.

3. Reduction

In the case of a failure to comply which is due to reasonable cause and not to willful neglect, any penalty under subsection (a) and any damages under subsection (d) that is [2] not entirely waived under paragraph (3) may be waived to the extent that the payment of such penalty would be excessive relative to the compliance failure involved.

c. Noncompliance due to willful neglect

1. In general

A violation of a provision of this part due to willful neglect is a violation for which the Secretary is required to impose a penalty under subsection (a)(1).

2. Required investigation

For purposes of paragraph (1), the Secretary shall formally investigate any complaint of a violation of a provision of this part if a preliminary investigation of the facts of the complaint indicate such a possible violation due to willful neglect.

d. Enforcement by State attorneys general

1. Civil action

   Except as provided in subsection (b), in any case in which the attorney general of a State 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, the attorney general of the State, as parens patriae, may bring a civil action on behalf of such residents of the State in a district court of the United States of appropriate jurisdiction—

   A. to enjoin further such violation by the defendant; or

   B. to obtain damages on behalf of such residents of the State, in an amount equal to the amount determined under paragraph (2).

2. Statutory damages

   A. In general

      For purposes of paragraph (1)(B), the amount determined under this paragraph is the amount calculated by multiplying the number of violations by up to $100. For purposes of the preceding sentence, in the case of a continuing violation, the number of violations shall be determined consistent with the HIPAA privacy regulations (as defined in section 1320d–9(b)(3) of this title) for violations of subsection (a).

   B. Limitation

      The total amount of damages imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.

   C. Reduction of damages

      In assessing damages under subparagraph (A), the court may consider the factors the Secretary may consider in determining the amount of a civil money penalty under subsection (a) under the HIPAA privacy regulations.

3. Attorney fees

   In the case of any successful action under paragraph (1), the court, in its discretion, may award the costs of the action and reasonable attorney fees to the State.

4. Notice to Secretary

   The State shall serve prior written notice of any action under paragraph

(1) upon the Secretary and provide the Secretary with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon instituting such action. The Secretary shall have the right—

A. to intervene in the action;

B. upon so intervening, to be heard on all matters arising therein; and

C. to file petitions for appeal.

5. Construction

For purposes of bringing any civil action under paragraph (1), nothing in this section shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State.

6. Venue; service of process

A. Venue

Any action brought under paragraph (1) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28.

B. Service of process

In an action brought under paragraph (1), process may be served in any district in which the defendant—

i. is an inhabitant; or

ii. maintains a physical place of business.

7. Limitation on State action while Federal action is pending

If the Secretary has instituted an action against a person under subsection (a) with respect to a specific violation of this part, no State attorney general may bring an action under this subsection against the person with respect to such violation during the pendency of that action.

8. Application of CMP statute of limitation

A civil action may not be instituted with respect to a violation of this part unless an action to impose a civil money penalty may be instituted under subsection (a) with respect to such violation consistent with the second sentence of section 1320a–7a(c)(1) of this title.

e. Allowing continued use of corrective action

Nothing in this section shall be construed as preventing the Office for Civil Rights of the Department of Health and Human Services from continuing, in its discretion, to use corrective action without a penalty in cases where the person did not know (and by exercising reasonable diligence would not have known) of the violation involved.[15]

Context: Before the HITECH Act, HIPAA violations were relatively mild, with each violation limited to $100 and totaling no more than $25,000 per calendar year. The HITECH Act imposed a more complex penalty scheme with much tougher potential penalties. Penalties for violations occurring after the HITECH Act's passage may range from $100 to $10,000 per violation with the total aggregate limit of $1.5 million per calendar year. Further, the penalties are subject to yearly adjustments according to inflation. Current penalty amounts are found at 45 C.F.R. § 102.3 .