42 USC Ch. 156: HEALTH INFORMATION TECHNOLOGY

From Title 42—THE PUBLIC HEALTH AND WELFARE

CHAPTER 156—HEALTH INFORMATION TECHNOLOGY

SUBCHAPTER I—APPLICATION AND USE OF ADOPTED HEALTH INFORMATION TECHNOLOGY STANDARDS; REPORTS

SUBCHAPTER I—APPLICATION AND USE OF ADOPTED HEALTH INFORMATION TECHNOLOGY STANDARDS; REPORTS

§17901. Coordination of Federal activities with adopted standards and implementation specifications

(a) Spending on health information technology systems

As each agency (as defined by the Director of the Office of Management and Budget, in consultation with the Secretary of Health and Human Services) implements, acquires, or upgrades health information technology systems

used for the direct exchange of individually identifiable health information between agencies and with non-Federal entities, it shall utilize, where available, health information technology systems and products that meet standards and implementation specifications adopted under section 300jj–14 of this title, as added by section 13101.[1]

(b) Federal information collection activities

With respect to a standard or implementation specification adopted under section 300jj–14 of this title, as added by section 13101, the President shall take measures to ensure that Federal activities involving the broad collection and submission of health information are consistent with such standard or implementation specification, respectively, within three years after the date of such adoption.

(c) Application of definitions

The definitions contained in section 300jj of this title, as added by section 13101,[1] shall apply for purposes of this subchapter.

(Pub. L. 111–5, div. A, title XIII, §13111, Feb. 17, 2009, 123 Stat. 242.)

References in Text

Section 13101, referred to in text, means section 13101 of div. A of Pub. L. 111–5.

[1] *See References in Text note below.*

§17902. Application to private entities

Each agency (as defined in such Executive Order issued on August 22, 2006, relating to promoting quality and efficient health care in Federal government administered or sponsored health care programs) shall require in contracts or agreements with health care providers, health plans, or health insurance issuers that as each provider, plan, or issuer implements, acquires, or upgrades health information technology systems, it shall utilize, where available, health information technology systems and products that meet standards and implementation specifications adopted under section 300jj–14 of this title, as added by section 13101.[1]

(Pub. L. 111–5, div. A, title XIII, §13112, Feb. 17, 2009, 123 Stat. 243.)

References in Text

Executive Order issued on August 22, 2006, referred to in text, is Ex. Ord. No. 13410, Aug. 22, 2006, 71 F.R. 51089, which is set out as a note under section 300u of this title.

Section 13101, referred to in text, means section 13101 of div. A of Pub. L. 111–5.

[1] *See References in Text note below.*

§17903. Study and reports

(a) Report on adoption of nationwide system

Not later than 2 years after February 17, 2009, and annually thereafter, the Secretary of Health and Human Services shall submit to the appropriate committees of jurisdiction of the House of Representatives and the Senate a report that —

(1) describes the specific actions that have been taken by the Federal Government and private entities to facilitate the adoption of a nationwide system for the electronic use and exchange of health information;

(2) describes barriers to the adoption of such a nationwide system; and

(3) contains recommendations to achieve full implementation of such a nationwide system.

(b) Reimbursement incentive study and report

(1) Study

The Secretary of Health and Human Services shall carry out, or contract with a private entity to carry out, a study that examines methods to create efficient reimbursement incentives for improving health care quality in Federally qualified health centers, rural health clinics, and free clinics.

(2) Report

Not later than 2 years after February 17, 2009, the Secretary of Health and Human Services shall submit to the appropriate committees of jurisdiction of the House of Representatives and the Senate a report on the study carried out under paragraph (1).

(c) Aging services technology study and report

(1) In general

The Secretary of Health and Human Services shall carry out, or contract with a private entity to carry out, a study of matters relating to the potential use of new aging services technology to assist seniors, individuals with disabilities, and their caregivers throughout the aging process.

(2) Matters to be studied

The study under paragraph (1) shall include—

(A) an evaluation of—

(i) methods for identifying current, emerging, and future health technology that can be used to meet the needs of seniors and individuals with disabilities and their caregivers across all aging services settings, as specified by the Secretary;

(ii) methods for fostering scientific innovation with respect to aging services technology within the business and academic communities; and

(iii) developments in aging services technology in other countries that may be applied in the United States; and

(B) identification of—

(i) barriers to innovation in aging services technology and devising strategies for removing such barriers; and

(ii) barriers to the adoption of aging services technology by health care providers and consumers and devising strategies to removing such barriers.

(3) Report

Not later than 24 months after February 17, 2009, the Secretary shall submit to the appropriate committees of jurisdiction of the House of Representatives and of the Senate a report on the study carried out under paragraph (1).

(4) Definitions

For purposes of this subsection:

(A) Aging services technology

The term "aging services technology" means health technology that meets the health care needs of seniors, individuals with disabilities, and the caregivers of such seniors and individuals.

(B) Senior

The term "senior" has such meaning as specified by the Secretary.

(Pub. L. 111–5, div. A, title XIII, §13113, Feb. 17, 2009, 123 Stat. 243.)

SUBCHAPTER II—TESTING OF HEALTH INFORMATION TECHNOLOGY

§17911. National Institute for Standards and Technology testing

(a) Pilot testing of standards and implementation specifications

In coordination with the HIT Standards Committee established under section 300jj–13 [1] of this title, as added by section 13101,[1] with respect to the development of standards and implementation specifications under such section, the Director of the National Institute for Standards and Technology shall test such standards and implementation specifications, as appropriate, in order to assure the efficient implementation and use of such standards and implementation specifications.

(b) Voluntary testing program

In coordination with the HIT Standards Committee established under section 300jj–13 [1] of this title, as added by section 13101,[1] with respect to the development of standards and implementation specifications under such section, the Director of the National Institute of Standards and Technology shall support the establishment of a conformance testing infrastructure, including the development of technical test beds. The development of this conformance testing infrastructure may include a program to accredit independent, non-Federal laboratories to perform testing.

(Pub. L. 111–5, div. A, title XIII, §13201, Feb. 17, 2009, 123 Stat. 244.)

References in Text

Section 300jj–13 of this title, referred to in text, which related to the establishment of the HIT Standards Committee, was repealed by Pub. L. 114–255, div. A, title IV, §4003(e)(1), Dec. 13, 2016, 130 Stat. 1168.

Section 13101, referred to in text, means section 13101 of div. A of Pub. L. 111–5.

[1] *See References in Text note below.*

§17912. Research and development programs

(a) Health Care Information Enterprise Integration Research Centers

(1) In general

The Director of the National Institute of Standards and Technology, in consultation with the Director of the National Science Foundation and other appropriate Federal agencies, shall establish a program of assistance to institutions of higher education (or consortia thereof which may include nonprofit entities and Federal Government laboratories) to establish multidisciplinary Centers for Health Care Information Enterprise Integration.

(2) Review; competition

Grants shall be awarded under this subsection on a merit-reviewed, competitive basis.

(3) Purpose

The purposes of the Centers described in paragraph (1) shall be—

(A) to generate innovative approaches to health care information enterprise integration by conducting cutting-edge, multidisciplinary research on the systems challenges to health care delivery; and

(B) the development and use of health information technologies and other complementary fields.

(4) Research areas

Research areas may include—

(A) interfaces between human information and communications technology systems;

(B) voice-recognition systems;

(C) software that improves interoperability and connectivity among health information systems;

(D) software dependability in systems critical to health care delivery;

(E) measurement of the impact of information technologies on the quality and productivity of health care;

(F) health information enterprise management;

(G) health information technology security and integrity; and

(H) relevant health information technology to reduce medical errors.

(5) Applications

An institution of higher education (or a consortium thereof) seeking funding under this subsection shall submit an application to the Director of the National Institute of Standards and Technology at such time, in such manner, and containing such information as the Director may require. The application shall include, at a minimum, a description of—

(A) the research projects that will be undertaken by the Center established pursuant to assistance under paragraph (1) and the respective contributions of the participating entities;

(B) how the Center will promote active collaboration among scientists and engineers from different disciplines, such as information technology, biologic sciences, management, social sciences, and other appropriate disciplines;

(C) technology transfer activities to demonstrate and diffuse the research results, technologies, and knowledge; and

(D) how the Center will contribute to the education and training of researchers and other professionals in fields relevant to health information enterprise integration.

(b) National information technology research and development program

The Networking and Information Technology Research and Development Program established by section 5511 of title 15 shall include Federal research and development programs related to health information technology.

(Pub. L. 111–5, div. A, title XIII, §13202, Feb. 17, 2009, 123 Stat. 245; Pub. L. 114–329, title I, §105(s), Jan. 6, 2017, 130 Stat. 2985.)

AMENDMENTS

2017—Subsec. (b). Pub. L. 114–329 substituted "Networking and Information Technology Research and Development Program" for "National High-Performance Computing Program".

SUBCHAPTER III—PRIVACY

§17921. Definitions

In this subchapter, except as specified otherwise:

(1) Breach

(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 [1] 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.

(2) Business associate

The term "business associate" has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(3) Covered entity

The term "covered entity" has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(4) Disclose

The terms "disclose" and "disclosure" have the meaning given the term "disclosure" in section 160.103 of title 45, Code of Federal Regulations.

(5) Electronic health record

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.

(6) Health care operations

The term "health care operation" has the meaning given such term in section 164.501 of title 45, Code of Federal Regulations.

(7) Health care provider

The term "health care provider" has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(8) Health plan

The term "health plan" has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(9) National Coordinator

The term "National Coordinator" means the head of the Office of the National Coordinator for Health Information Technology established under section 300jj–11(a) of this title, as added by section 13101.[2]

(10) Payment

The term "payment" has the meaning given such term in section 164.501 of title 45, Code of Federal Regulations.

(11) Personal health record

The term "personal health record" means an electronic record of PHR identifiable health information (as defined in section 17937(f)(2) of this title) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

(12) Protected health information

The term "protected health information" has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(13) Secretary

The term "Secretary" means the Secretary of Health and Human Services.

(14) Security

The term "security" has the meaning given such term in section 164.304 of title 45, Code of Federal Regulations.

(15) State

The term "State" means each of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.

(16) Treatment

The term "treatment" has the meaning given such term in section 164.501 of title 45, Code of Federal Regulations.

(17) Use

The term "use" has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(18) Vendor of personal health records

The term "vendor of personal health records" means an entity, other than a covered entity (as defined in paragraph (3)), that offers or maintains a personal health record.

(Pub. L. 111–5, div. A, title XIII, §13400, Feb. 17, 2009, 123 Stat. 258.)

References in Text

This subchapter, referred to in text, was in the original "this subtitle", meaning subtitle D (§13400 et seq.) of title XIII of div. A of Pub. L. 111–5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this subchapter. For complete classification of subtitle D to the Code, see Tables.

Section 13101, referred to in par. (9), means section 13101 of div. A of Pub. L. 111–5.

[1] *So in original. Probably should be followed by "the".*

[2] *See References in Text note below.*

Part A—Improved Privacy Provisions and Security Provisions

§17931. Application of security provisions and penalties to business associates of covered entities; annual guidance on security provisions

(a) Application of security provisions

Sections 164.308, 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity. The additional requirements of this title [1] that relate to security 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 civil and criminal penalties

In the case of a business associate that violates any security provision specified in subsection (a), sections 1320d–5 and 1320d–6 of this title shall apply to the business associate with respect to such violation in the same manner such sections apply to a covered entity that violates such security provision.

(c) Annual guidance

For the first year beginning after February 17, 2009, and annually thereafter, the Secretary of Health and Human Services shall, after consultation with stakeholders, annually issue guidance on the most effective and appropriate technical safeguards for use in carrying out the sections referred to in subsection (a) and the security standards in subpart C of part 164 of title 45, Code of Federal Regulations, including the use of standards developed under section 300jj–12(b)(2)(B)(vi) [1] of this title, as added by section 13101 of this Act, as such provisions are in effect as of the date before February 17, 2009.

(Pub. L. 111–5, div. A, title XIII, §13401, Feb. 17, 2009, 123 Stat. 260.)

References in Text

This title, referred to in subsec. (a), is title XIII of div. A of Pub. L. 111–5, which enacted this chapter and subchapter XXVIII (§300jj et seq.) of chapter 6A this title, amended sections 1320d, 1320d–5, and 1320d–6 of this title, and enacted provisions set out as a note under this section and section 201 of this title. For

complete classification of title XIII to the Code, see Short Title of 2009 Amendment note set out under section 201 of this title and Tables.

Section 300jj–12(b)(2)(B)(vi) of this title, referred to in subsec. (c), was repealed by Pub. L. 114–255, div. A, title IV, §4003(e)(1), Dec. 13, 2016, 130 Stat. 1168. Similar provisions as pertaining to the HIT Advisory Committee are contained in section 300jj–12(b)(2)(C)(vii) of this title as enacted by Pub. L. 114–255.

Section 13101 of this Act, referred to in subsec. (c), means section 13101 of div. A of Pub. L. 111–5.

Effective Date

Pub. L. 111–5, div. A, title XIII, §13423, Feb. 17, 2009, 123 Stat. 276, provided that: "Except as otherwise specifically provided, the provisions of part I [probably means part 1 (§§13401–13411) of subtitle D of title XIII of div. A of Pub. L. 111–5, enacting this part and amending sections 1320d–5 and 1320d–6 of this title] shall take effect on the date that is 12 months after the date of the enactment of this title [Feb. 17, 2009]."

[1] *See References in Text note below.*

§17932. Notification in the case 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 [1] 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) [2] 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.

(Pub. L. 111–5, div. A, title XIII, §13402, Feb. 17, 2009, 123 Stat. 260.)

References in Text

Section 300jj–12(b)(2)(B)(vi) of this title, referred to in subsec. (h)(2), was repealed by Pub. L. 114–255, div. A, title IV, §4003(e)(1), Dec. 13, 2016, 130 Stat. 1168. Similar provisions as pertaining to the HIT Advisory Committee are contained in section 300jj–12(b)(2)(C)(vii) of this title as enacted by Pub. L. 114–255.

Section 13101 of this Act, referred to in subsec. (h)(2), means section 13101 of div. A of Pub. L. 111–5.

Effective Date

Section effective 12 months after Feb. 17, 2009, except as otherwise specifically provided, see section 13423 of Pub. L. 111–5, set out as a note under section 17931 of this title.

[1] *So in orginal. Probably should be "then".*

[2] *See References in Text note below.*

§17933. Education on health information privacy

(a) Regional office privacy advisors

Not later than 6 months after February 17, 2009, the Secretary shall designate an individual in each regional office of the Department of Health and Human Services to offer guidance and education to covered entities, business associates, and individuals on their rights and responsibilities related to Federal privacy and security requirements for protected health information.

(b) Education initiative on uses of health information

Not later than 12 months after February 17, 2009, the Office for Civil Rights within the Department of Health and Human Services shall develop and maintain a multi-faceted national education initiative to enhance public transparency regarding the uses of protected health information, including programs to educate individuals about the potential uses of their protected health information, the effects of such uses, and the rights of individuals with respect to such uses. Such programs shall be conducted in a variety of languages and present information in a clear and understandable manner.

(Pub. L. 111–5, div. A, title XIII, §13403, Feb. 17, 2009, 123 Stat. 263.)

Effective Date

Section effective 12 months after Feb. 17, 2009, except as otherwise specifically provided, see section 13423 of Pub. L. 111–5, set out as a note under section 17931 of this title.

§17934. Application of privacy provisions and penalties to business associates of covered entities

(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.].

(Pub. L. 111–5, div. A, title XIII, §13404, Feb. 17, 2009, 123 Stat. 264.)

References in Text

This subchapter, referred to in subsec. (a), was in the original "this subtitle", meaning subtitle D (§13400 et seq.) of title XIII of div. A of Pub. L. 111–5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this subchapter. For complete classification of subtitle D to the Code, see Tables.

The Social Security Act, referred to in subsec. (c), is act Aug. 14, 1935, ch. 531, 49 Stat. 620. Part C of title XI of the Act is classified generally to part C (§1320d et seq.) of subchapter XI of chapter 7 of this title. For complete classification of this Act to the Code, see section 1305 of this title and Tables.

Effective Date

Section effective 12 months after Feb. 17, 2009, except as otherwise specifically provided, see section 13423 of Pub. L. 111–5, set out as a note under section 17931 of this title.

§17935. Restrictions on certain disclosures and sales of health information; accounting of certain protected health information disclosures; access to certain information in electronic format

(a) Requested restrictions on certain disclosures of health information

In the case that an individual requests under paragraph (a)(1)(i)(A) of section 164.522 of title 45, Code of Federal Regulations, that a covered entity restrict the disclosure of the protected health information of the individual, notwithstanding paragraph (a)(1)(ii) of such section, the covered entity must comply with the requested restriction if—

(1) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and

(2) the protected health information pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

(b) Disclosures required to be limited to the limited data set or the minimum necessary

(1) In general

(A) In general

Subject to subparagraph (B), a covered entity shall be treated as being in compliance with section 164.502(b)(1) of title 45, Code of Federal Regulations, with respect to the use, disclosure, or request of protected health information described in such section, only if the covered entity limits such protected health information, to the extent practicable, to the limited data set (as defined in section 164.514(e)(2) of such title) or, if needed by such entity, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request, respectively.

(B) Guidance

Not later than 18 months after February 17, 2009, the Secretary shall issue guidance on what constitutes "minimum necessary" for purposes of subpart E of part 164 of title 45, Code of Federal Regulation.[1] In issuing such guidance the Secretary shall take into consideration the guidance under section 17953(c) of this title and the information necessary to improve patient outcomes and to detect, prevent, and manage chronic disease.

(C) Sunset

Subparagraph (A) shall not apply on and after the effective date on which the Secretary issues the guidance under subparagraph (B).

(2) Determination of minimum necessary

For purposes of paragraph (1), in the case of the disclosure of protected health information, the covered entity or business associate disclosing such information shall determine what constitutes the minimum necessary to accomplish the intended purpose of such disclosure.

(3) Application of exceptions

The exceptions described in section 164.502(b)(2) of title 45, Code of Federal Regulations, shall apply to the requirement under paragraph (1) as of the effective date described in section 13423 [2] in the same manner that such exceptions apply to section 164.502(b)(1) of such title before such date.

(4) Rule of construction

Nothing in this subsection shall be construed as affecting the use, disclosure, or request of protected health information that has been de-identified.

(c) Accounting of certain protected health information disclosures required if covered entity uses electronic health record

(1) In general

In applying section 164.528 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—

(A) the exception under paragraph (a)(1)(i) of such section shall not apply to disclosures through an electronic health record made by such entity of such information; and

(B) an individual shall have a right to receive an accounting of disclosures described in such paragraph of such information made by such covered entity during only the three years prior to the date on which the accounting is requested.

(2) Regulations

The Secretary shall promulgate regulations on what information shall be collected about each disclosure referred to in paragraph (1), not later than 6 months after the date on which the Secretary adopts standards on accounting for disclosure described in the [3] section 300jj–12(b)(2)(B)(iv) of this title, as added by section 13101.[2] Such regulations shall only require such information to be collected through an electronic health record in a manner that takes into account the interests of the individuals in learning the circumstances under which their protected health information is being disclosed and takes into account the administrative burden of accounting for such disclosures.

(3) Process

In response to an [4] request from an individual for an accounting, a covered entity shall elect to provide either an—

(A) accounting, as specified under paragraph (1), for disclosures of protected health information that are made by such covered entity and by a business associate acting on behalf of the covered entity; or

(B) accounting, as specified under paragraph (1), for disclosures that are made by such covered entity and provide a list of all business associates acting on behalf of the covered entity, including contact information for such associates (such as mailing address, phone, and email address).

A business associate included on a list under subparagraph (B) shall provide an accounting of disclosures (as required under paragraph (1) for a covered entity) made by the business associate upon a request made by an individual directly to the business associate for such an accounting.

(4) Effective date

(A) Current users of electronic records

In the case of a covered entity insofar as it acquired an electronic health record as of January 1, 2009, paragraph (1) shall apply to disclosures, with respect to protected health information, made by the covered entity from such a record on and after January 1, 2014.

(B) Others

In the case of a covered entity insofar as it acquires an electronic health record after January 1, 2009, paragraph (1) shall apply to disclosures, with respect to protected health information, made by the covered entity from such record on and after the later of the following:

(i) January 1, 2011; or

(ii) the date that it acquires an electronic health record.

(C) Later date

The Secretary may set an effective date that is later that [5] the date specified under subparagraph (A) or (B) if the Secretary determines that such later date is necessary, but in no case may the date specified under—

(i) subparagraph (A) be later than 2016; or

(ii) subparagraph (B) be later than 2013.

(d) Prohibition on sale of electronic health records or protected health information

(1) In general

Except as provided in paragraph (2), a covered entity or business associate shall not directly or indirectly receive remuneration in exchange for any protected health information of an individual unless the covered entity obtained from the individual, in accordance with section 164.508 of title 45, Code of Federal Regulations, a valid authorization that includes, in accordance with such section, a specification of whether the protected health information can be further exchanged for remuneration by the entity receiving protected health information of that individual.

(2) Exceptions

Paragraph (1) shall not apply in the following cases:

(A) The purpose of the exchange is for public health activities (as described in section 164.512(b) of title 45, Code of Federal Regulations).

(B) The purpose of the exchange is for research (as described in sections 164.501 and 164.512(i) of title 45, Code of Federal Regulations) and the price charged reflects the costs of preparation and transmittal of the data for such purpose.

(C) The purpose of the exchange is for the treatment of the individual, subject to any regulation that the Secretary may promulgate to prevent protected health information from inappropriate access, use, or disclosure.

(D) The purpose of the exchange is the health care operation specifically described in subparagraph (iv) of paragraph (6) of the definition of healthcare operations in section 164.501 of title 45, Code of Federal Regulations.

(E) The purpose of the exchange is for remuneration that is provided by a covered entity to a business associate for activities involving the exchange of protected health information that the business associate undertakes on behalf of and at the specific request of the covered entity pursuant to a business associate agreement.

(F) The purpose of the exchange is to provide an individual with a copy of the individual's protected health information pursuant to section 164.524 of title 45, Code of Federal Regulations.

(G) The purpose of the exchange is otherwise determined by the Secretary in regulations to be similarly necessary and appropriate as the exceptions provided in subparagraphs (A) through (F).

(3) Regulations

Not later than 18 months after February 17, 2009, the Secretary shall promulgate regulations to carry out this subsection. In promulgating such regulations, the Secretary—

(A) shall evaluate the impact of restricting the exception described in paragraph (2)(A) to require that the price charged for the purposes described in such paragraph reflects the costs of the preparation and transmittal of the data for such purpose, on research or public health activities, including those conducted by or for the use of the Food and Drug Administration; and

(B) may further restrict the exception described in paragraph (2)(A) to require that the price charged for the purposes described in such paragraph reflects the costs of the preparation and transmittal of the data for such purpose, if the Secretary finds that such further restriction will not impede such research or public health activities.

(4) Effective date

Paragraph (1) shall apply to exchanges occurring on or after the date that is 6 months after the date of the promulgation of final regulations implementing this subsection.

(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).

(Pub. L. 111–5, div. A, title XIII, §13405, Feb. 17, 2009, 123 Stat. 264; Pub. L. 114–255, div. A, title IV, §4006(b), Dec. 13, 2016, 130 Stat. 1183.)

References in Text

Section 13423, referred to in subsec. (b)(3), means section 13423 of div. A of Pub. L. 111–5, which is set out as an Effective Date note under section 17931 of this title.

Section 300jj–12(b)(2)(B)(iv) of this title, as added by section 13101, referred to in subsec. (c)(2), means section 300jj–12(b)(2)(B)(iv) of this title as added by section 13101 of div. A of Pub. L. 111–5. Section 300jj–12 of

this title was repealed by Pub. L. 114–255, div. A, title IV, §4003(e)(1), Dec. 13, 2016, 130 Stat. 1168. Similar provisions as pertaining to the HIT Advisory Committee are contained in section 300jj–12(b)(2)(B)(ii) of this title as enacted by Pub. L. 114–255.

Amendments

2016—Subsec. (e)(2), (3). Pub. L. 114–255 added par. (2) and redesignated former par. (2) as (3).

Effective Date

Section effective 12 months after Feb. 17, 2009, except as otherwise specifically provided, see section 13423 of Pub. L. 111–5, set out as a note under section 17931 of this title.

[1] *So in original. Probably should be "Regulations."*

[2] *See References in Text note below.*

[3] *So in original.*

[4] *So in original. Probably should be "a".*

[5] *So in original. Probably should be "than".*

§17936. Conditions on certain contacts as part of health care operations

(a) Marketing

(1) In general

A communication by a covered entity or business associate that is about a product or service and that encourages recipients of the communication to purchase or use the product or service shall not be considered a health care operation for purposes of subpart E of part 164 of title 45, Code of Federal Regulations, unless the communication is made as described in subparagraph (i), (ii), or (iii) of paragraph (1) of the definition of marketing in section 164.501 of such title.

(2) Payment for certain communications

A communication by a covered entity or business associate that is described in subparagraph (i), (ii), or (iii) of paragraph (1) of the definition of marketing in section 164.501 of title 45, Code of Federal Regulations, shall not be considered a health care operation for purposes of subpart E of part 164 of title 45, Code of Federal Regulations if the covered entity receives or has received direct or indirect payment in exchange for making such communication, except where—

(A)(i) such communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication; and

(ii) any payment received by such covered entity in exchange for making a communication described in clause (i) is reasonable in amount;

(B) each of the following conditions apply—

(i) the communication is made by the covered entity; and

(ii) the covered entity making such communication obtains from the recipient of the communication, in accordance with section 164.508 of title 45, Code of Federal Regulations, a valid authorization (as described in paragraph (b) of such section) with respect to such communication; or

(C) each of the following conditions apply—

(i) the communication is made by a business associate on behalf of the covered entity; and

(ii) the communication is consistent with the written contract (or other written arrangement described in section 164.502(e)(2) of such title) between such business associate and covered entity.

(3) Reasonable in amount defined

For purposes of paragraph (2), the term "reasonable in amount" shall have the meaning given such term by the Secretary by regulation.

(4) Direct or indirect payment

For purposes of paragraph (2), the term "direct or indirect payment" shall not include any payment for treatment (as defined in section 164.501 of title 45, Code of Federal Regulations) of an individual.

(b) Opportunity to opt out of fundraising

The Secretary shall by rule provide that any written fundraising communication that is a healthcare operation as defined under section 164.501 of title 45, Code of Federal Regulations, shall, in a clear and conspicuous manner, provide an opportunity for the recipient of the communications to elect not to receive any further such communication. When an individual elects not to receive any further such communication, such election shall be treated as a revocation of authorization under section 164.508 of title 45, Code of Federal Regulations.

(c) Effective date

This section shall apply to written communications occurring on or after the effective date specified under section 13423.[1]

(Pub. L. 111–5, div. A, title XIII, §13406, Feb. 17, 2009, 123 Stat. 268.)

References in Text

Section 13423, referred to in subsec. (c), means section 13423 of div. A of Pub. L. 111–5, which is set out as an Effective Date note under section 17931 of this title.

Effective Date

Section effective 12 months after Feb. 17, 2009, except as otherwise specifically provided, see section 13423 of Pub. L. 111–5, set out as a note under section 17931 of this title.

[1] *See References in Text note below.*

§17937. Temporary breach notification requirement for vendors of personal health records and other non-HIPAA covered entities

(a) In general

In accordance with subsection (c), each vendor of personal health records, following the discovery of a breach of security of unsecured PHR identifiable health information that is in a personal health record maintained or offered by such vendor, and each entity described in clause (ii), (iii), or (iv) of section 17953(b)(1)(A) of this title, following the discovery of a breach of security of such information that is obtained through a product or service provided by such entity, shall—

(1) notify each individual who is a citizen or resident of the United States whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of such a breach of security; and

(2) notify the Federal Trade Commission.

(b) Notification by third party service providers

A third party service provider that provides services to a vendor of personal health records or to an entity described in clause (ii), (iii).[1] or (iv) of section 17953(b)(1)(A) of this title in connection with the offering or maintenance of a personal health record or a related product or service and that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information in such a record as a result of such services shall, following the discovery of a breach of security of such information, notify such vendor or entity, respectively, of such breach. Such notice shall include the identification of each individual whose unsecured PHR identifiable health information has been, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

(c) Application of requirements for timeliness, method, and content of notifications

Subsections (c), (d), (e), and (f) of section 17932 of this title shall apply to a notification required under subsection (a) and a vendor of personal health records, an entity described in subsection (a) and a third party service provider described in subsection (b), with respect to a breach of security under subsection (a) of unsecured PHR identifiable health information in such records maintained or offered by such vendor, in a manner specified by the Federal Trade Commission.

(d) Notification of the Secretary

Upon receipt of a notification of a breach of security under subsection (a)(2), the Federal Trade Commission shall notify the Secretary of such breach.

(e) Enforcement

A violation of subsection (a) or (b) shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 57a(a)(1)(B) of title 15 regarding unfair or deceptive acts or practices.

(f) Definitions

For purposes of this section:

(1) Breach of security

The term "breach of security" means, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual.

(2) PHR identifiable health information

The term "PHR identifiable health information" means individually identifiable health information, as defined in section 1320d(6) of this title, and includes, with respect to an individual, information—

(A) that is provided by or on behalf of the individual; and

(B) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

(3) Unsecured PHR identifiable health information

(A) In general

Subject to subparagraph (B), the term "unsecured PHR identifiable health information" means PHR identifiable health information that is not protected through the use of a technology or methodology specified by the Secretary in the guidance issued under section 17932(h)(2) of this title.

(B) Exception in case timely guidance not issued

In the case that the Secretary does not issue guidance under section 17932(h)(2) of this title by the date specified in such section, for purposes of this section, the term "unsecured PHR identifiable health information" shall mean PHR identifiable health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and that is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

(g) Regulations; effective date; sunset

(1) Regulations; effective date

To carry out this section, the Federal Trade Commission 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 of security that are discovered on or after the date that is 30 days after the date of publication of such interim final regulations.

(2) Sunset

If Congress enacts new legislation establishing requirements for notification in the case of a breach of security, that apply to entities that are not covered entities or business associates, the provisions of this section shall not apply to breaches of security discovered on or after the effective date of regulations implementing such legislation.

(Pub. L. 111–5, div. A, title XIII, §13407, Feb. 17, 2009, 123 Stat. 269.)

Effective Date

Section effective 12 months after Feb. 17, 2009, except as otherwise specifically provided, see section 13423 of Pub. L. 111–5, set out as a note under section 17931 of this title.

[1] *So in original. The period probably should be a comma.*

§17938. Business associate contracts required for certain entities

Each organization, with respect to a covered entity, that provides data transmission of protected health information to such entity (or its business associate) and that requires access on a routine basis to such protected health information, such as a Health Information Exchange Organization, Regional Health Information Organization, E-prescribing Gateway, or each vendor that contracts with a covered entity to allow that covered entity to offer a personal health record to patients as part of its electronic health record, is required to enter into a written contract (or other written arrangement) described in section 164.502(e)(2) of title 45, Code of Federal Regulations and a written contract (or other arrangement) described in section 164.308(b) of such title, with such entity and shall be treated as a business associate of the covered entity for purposes of the provisions of this subchapter and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of February 17, 2009.

(Pub. L. 111–5, div. A, title XIII, §13408, Feb. 17, 2009, 123 Stat. 271.)

References in Text

This subchapter, referred to in text, was in the original "this subtitle", meaning subtitle D (§13400 et seq.) of title XIII of div. A of Pub. L. 111–5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this subchapter. For complete classification of subtitle D to the Code, see Tables.

Effective Date

Section effective 12 months after Feb. 17, 2009, except as otherwise specifically provided, see section 13423 of Pub. L. 111–5, set out as a note under section 17931 of this title.

§17939. Improved enforcement

(a) In general

(1) Omitted

(2) Enforcement under Social Security Act

Any violation by a covered entity under thus [1] subchapter is subject to enforcement and penalties under section [2] 1176 and 1177 of the Social Security Act [42 U.S.C. 1320d–5, 1320d–6].

(b) Effective date; regulations

(1) The amendments made by subsection (a) shall apply to penalties imposed on or after the date that is 24 months after February 17, 2009.

(2) Not later than 18 months after February 17, 2009, the Secretary of Health and Human Services shall promulgate regulations to implement such amendments.

(c) Distribution of certain civil monetary penalties collected

(1) In general

Subject to the regulation promulgated pursuant to paragraph (3), any civil monetary penalty or monetary settlement collected with respect to an offense punishable under this subchapter or section 1176 of the Social Security Act (42 U.S.C. 1320d–5) insofar as such section relates to privacy or security shall be transferred to the Office for Civil Rights of the Department of Health and Human Services to be used for purposes of enforcing the provisions of this subchapter and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of February 17, 2009.

(2) GAO report

Not later than 18 months after February 17, 2009, the Comptroller General shall submit to the Secretary a report including recommendations for a methodology under which an individual who is harmed by an act that constitutes an offense referred to in paragraph (1) may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense.

(3) Establishment of methodology to distribute percentage of CMPS collected to harmed individuals

Not later than 3 years after February 17, 2009, the Secretary shall establish by regulation and based on the recommendations submitted under paragraph (2), a methodology under which an individual who is harmed by an act that constitutes an offense referred to in paragraph (1) may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense.

(4) Application of methodology

The methodology under paragraph (3) shall be applied with respect to civil monetary penalties or monetary settlements imposed on or after the effective date of the regulation.

(d) Tiered increase in amount of civil monetary penalties

(1) to (3) Omitted

(4) Effective date

The amendments made by this subsection shall apply to violations occurring after February 17, 2009.

(e) Enforcement through State attorneys general

(1), (2) Omitted

(3) Effective date

The amendments made by this subsection shall apply to violations occurring after February 17, 2009.

(Pub. L. 111–5, div. A, title XIII, §13410, Feb. 17, 2009, 123 Stat. 271.)

References in Text

This subchapter, referred to in subsecs. (a)(2) and (c)(1), was in the original "this subtitle", meaning subtitle D (§13400 et seq.) of title XIII of div. A of Pub. L. 111–5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this subchapter. For complete classification of subtitle D to the Code, see Tables.

For reference to "the amendments made by subsection (a)" in subsec. (b)(1) and "the amendments made by this subsection" in subsecs. (d)(4) and (e)(3), see Codification note below.

Codification

Section is comprised of section 13410 of Pub. L. 111–5. Subsecs. (a)(1), (d)(1)–(3), (e)(1), (2), and (f) of section 13410 of Pub. L. 111–5 amended section 1320d–5 of this title.

Effective Date

Section effective 12 months after Feb. 17, 2009, except as otherwise specifically provided, see section 13423 of Pub. L. 111–5, set out as a note under section 17931 of this title.

[1] *So in original. Probably should be "this".*

[2] *So in original. Probably should be "sections".*

§17940. Audits

The Secretary shall provide for periodic audits to ensure that covered entities and business associates that are subject to the requirements of this subchapter and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of February 17, 2009, comply with such requirements.

(Pub. L. 111–5, div. A, title XIII, §13411, Feb. 17, 2009, 123 Stat. 276.)

References in Text

This subchapter, referred to in text, was in the original "this subtitle", meaning subtitle D (§13400 et seq.) of title XIII of div. A of Pub. L. 111–5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this subchapter. For complete classification of subtitle D to the Code, see Tables.

Effective Date

Section effective 12 months after Feb. 17, 2009, except as otherwise specifically provided, see section 13423 of Pub. L. 111–5, set out as a note under section 17931 of this title.

§17941. Recognition of security practices

(a) In general

Consistent with the authority of the Secretary under sections 1320d–5 and 1320d–6 of this title, when making determinations relating to fines under such section 1320d–5 (as amended by section 13410 of Pub. L. 111–5) or such section 1320d–6, decreasing the length and extent of an audit under section 17940 of this title, or remedies otherwise agreed to by the Secretary, the Secretary shall consider whether the covered entity or business associate has adequately demonstrated that it had, for not less than the previous 12 months, recognized security practices in place that may—

(1) mitigate fines under section 1320d–5 of this title (as amended by section 13410 of Pub. L. 111–5);

(2) result in the early, favorable termination of an audit under section 17940 of this title; and

(3) mitigate the remedies that would otherwise be agreed to in any agreement with respect to resolving potential violations of the HIPAA Security rule (part 160 of title 45 Code of Federal Regulations and subparts A and C of part 164 of such title) between the covered entity or business associate and the Department of Health and Human Services.

(b) Definition and miscellaneous provisions

(1) Recognized security practices

The term "recognized security practices" means the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 272(c)(15) of title 15, the approaches promulgated under section 1533(d) of title 6, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities. Such practices shall be determined by the covered entity or business associate, consistent with the HIPAA Security rule (part 160 of title 45 Code of Federal Regulations and subparts A and C of part 164 of such title).

(2) Limitation

Nothing in this section shall be construed as providing the Secretary authority to increase fines under section 1320d–5 of this title (as amended by section 13410 of Pub. L. 111–5), or the length, extent or quantity of audits under section 17940 of this title, due to a lack of compliance with the recognized security practices.

(3) No liability for nonparticipation

Subject to paragraph (4), nothing in this section shall be construed to subject a covered entity or business associate to liability for electing not to engage in the recognized security practices defined by this section.

(4) Rule of construction

Nothing in this section shall be construed to limit the Secretary's authority to enforce the HIPAA Security rule (part 160 of title 45 Code of Federal Regulations and subparts A and C of part 164 of such title), or to supersede or

conflict with an entity or business associate's obligations under the HIPAA Security rule.

(Pub. L. 111–5, div. A, title XIII, §13412, as added Pub. L. 116–321, §1, Jan. 5, 2021, 134 Stat. 5072.)

Part B—Relationship to Other Laws; Regulatory References; Effective Date; Reports

§17951. Relationship to other laws

(a) Application of HIPAA State preemption

Section 1178 of the Social Security Act (42 U.S.C. 1320d–7) shall apply to a provision or requirement under this subchapter in the same manner that such section applies to a provision or requirement under part C of title XI of such Act [42 U.S.C. 1320d et seq.] or a standard or implementation specification adopted or established under sections 1172 through 1174 of such Act [42 U.S.C. 1320d–1 to 1320d–3].

(b) Health Insurance Portability and Accountability Act of 1996

The standards governing the privacy and security of individually identifiable health information promulgated by the Secretary under sections 262(a) and 264 of the Health Insurance Portability and Accountability Act of 1996 shall remain in effect to the extent that they are consistent with this subchapter. The Secretary shall by rule amend such Federal regulations as required to make such regulations consistent with this subchapter.

(c) Construction

Nothing in this subchapter shall constitute a waiver of any privilege otherwise applicable to an individual with respect to the protected health information of such individual.

(Pub. L. 111–5, div. A, title XIII, §13421, Feb. 17, 2009, 123 Stat. 276.)

References in Text

This subchapter, referred to in text, was in the original "this subtitle", meaning subtitle D (§13400 et seq.) of title XIII of div. A of Pub. L. 111–5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this subchapter. For complete classification of subtitle D to the Code, see Tables.

The Social Security Act, referred to in subsec. (a), is act Aug. 14, 1935, ch. 531, 49 Stat. 620. Part C of title XI of the Act is classified generally to part C (§1320d et seq.) of subchapter XI of chapter 7 of this title. For complete classification of this Act to the Code, see section 1305 of this title and Tables.

The Health Insurance Portability and Accountability Act of 1996, referred to in subsec. (b), is Pub. L. 104–191, Aug. 21, 1996, 110 Stat. 1936. Section 262(a) of the Act enacted sections 1320d to 1320d–8 of this title. Section 264 of the Act is set out as a note under section 1320d–2 of this title. For complete classification of this Act to the Code, see Short Title of 1996 Amendments note set out under section 201 of this title and Tables.

§17952. Regulatory references

Each reference in this subchapter to a provision of the Code of Federal Regulations refers to such provision as in effect on February 17, 2009 (or to the most recent update of such provision).

(Pub. L. 111–5, div. A, title XIII, §13422, Feb. 17, 2009, 123 Stat. 276.)

References in Text

This subchapter, referred to in text, was in the original "this subtitle", meaning subtitle D (§13400 et seq.) of title XIII of div. A of Pub. L. 111–5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this subchapter. For complete classification of subtitle D to the Code, see Tables.

§17953. Studies, reports, guidance

(a) Report on compliance

(1) In general

For the first year beginning after February 17, 2009, and annually thereafter, the Secretary shall prepare and submit to 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 concerning complaints of alleged violations of law, including the provisions of this subchapter as well as the provisions of

subparts C and E of part 164 of title 45, Code of Federal Regulations, (as such provisions are in effect as of February 17, 2009) relating to privacy and security of health information that are received by the Secretary during the year for which the report is being prepared. Each such report shall include, with respect to such complaints received during the year—

(A) the number of such complaints;

(B) the number of such complaints resolved informally, a summary of the types of such complaints so resolved, and the number of covered entities that received technical assistance from the Secretary during such year in order to achieve compliance with such provisions and the types of such technical assistance provided;

(C) the number of such complaints that have resulted in the imposition of civil monetary penalties or have been resolved through monetary settlements, including the nature of the complaints involved and the amount paid in each penalty or settlement;

(D) the number of compliance reviews conducted and the outcome of each such review;

(E) the number of subpoenas or inquiries issued;

(F) the Secretary's plan for improving compliance with and enforcement of such provisions for the following year; and

(G) the number of audits performed and a summary of audit findings pursuant to section 17940 of this title.

(2) Availability to public

Each report under paragraph (1) shall be made available to the public on the Internet website of the Department of Health and Human Services.

(b) Study and report on application of privacy and security requirements to non-HIPAA covered entities

(1) Study

Not later than one year after February 17, 2009, the Secretary, in consultation with the Federal Trade Commission, shall conduct a study, and submit a report under paragraph (2), on privacy and security requirements for entities that are not covered entities or business associates as of February 17, 2009, including—

(A) requirements relating to security, privacy, and notification in the case of a breach of security or privacy (including the applicability of an exemption to notification in the case of individually identifiable health information that has been rendered unusable, unreadable, or indecipherable through technologies or methodologies recognized by appropriate professional organization or standard setting bodies to provide effective security for the information) that should be applied to—

(i) vendors of personal health records;

(ii) entities that offer products or services through the website of a vendor of personal health records;

(iii) entities that are not covered entities and that offer products or services through the websites of covered entities that offer individuals personal health records;

(iv) entities that are not covered entities and that access information in a personal health record or send information to a personal health record; and

(v) third party service providers used by a vendor or entity described in clause (i), (ii), (iii), or (iv) to assist in providing personal health record products or services;

(B) a determination of which Federal government agency is best equipped to enforce such requirements recommended to be applied to such vendors, entities, and service providers under subparagraph (A); and

(C) a timeframe for implementing regulations based on such findings.

(2) Report

The Secretary shall submit to the Committee on Finance, the Committee on Health, Education, Labor, and Pensions, and the Committee on Commerce of the Senate and the Committee on Ways and Means and the Committee on Energy and Commerce of the House of Representatives a report on the findings of the study under paragraph (1) and shall include in such report recommendations on the privacy and security requirements described in such paragraph.

(c) Guidance on implementation specification to de-identify protected health information

Not later than 12 months after February 17, 2009, the Secretary shall, in consultation with stakeholders, issue guidance on how best to implement the requirements for the de-identification of protected health information under section 164.514(b) of title 45, Code of Federal Regulations.

(d) GAO report on treatment disclosures

Not later than one year after February 17, 2009, the Comptroller General of the United States shall submit to 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 on the best practices related to the disclosure among health care providers of protected health information of an individual for purposes of treatment of such individual. Such report shall include an examination of the best practices implemented by States and by other entities, such as health information exchanges and regional health information organizations, an examination of the extent to which such best practices are successful with respect to the quality of the resulting health care provided to the individual and with respect to the ability of the health care provider to manage such best practices, and an

examination of the use of electronic informed consent for disclosing protected health information for treatment, payment, and health care operations.

(e) Report required

Not later than 5 years after February 17, 2009, the Government Accountability Office shall submit to Congress and the Secretary of Health and Human Services a report on the impact of any of the provisions of this Act on health insurance premiums, overall health care costs, adoption of electronic health records by providers, and reduction in medical errors and other quality improvements.

(f) Study

The Secretary shall study the definition of "psychotherapy notes" in section 164.501 of title 45, Code of Federal Regulations, with regard to including test data that is related to direct responses, scores, items, forms, protocols, manuals, or other materials that are part of a mental health evaluation, as determined by the mental health professional providing treatment or evaluation in such definitions and may, based on such study, issue regulations to revise such definition.

(Pub. L. 111–5, div. A, title XIII, §13424, Feb. 17, 2009, 123 Stat. 276.)

References in Text

This subchapter, referred to in subsec. (a)(1), was in the original "this subtitle", meaning subtitle D (§13400 et seq.) of title XIII of div. A of Pub. L. 111–5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this subchapter. For complete classification of subtitle D to the Code, see Tables.

This Act, referred to in subsec. (e), means div. A of Pub. L. 111–5, Feb. 17, 2009, 123 Stat. 116, see section 4 of Pub. L. 111–5, set out as a note under section 1 of Title 1, General Provisions. For complete classification of div. A to the Code, see Tables.