

Subtitle D--Privacy

SEC. 13400. DEFINITIONS.

In this subtitle, 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 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 3001(a) of the Public Health Service Act, as added by section 13101.

(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 13407(f)(2)) 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.

#### PART 1--IMPROVED PRIVACY PROVISIONS AND SECURITY PROVISIONS

#### SEC. 13401. 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 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 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 such sections apply to a covered entity that violates such security provision.

(c) Annual Guidance.--For the first year beginning after the date of the enactment of this Act 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 3002(b)(2)(B)(vi) of the Public Health Service Act, as added by section 13101 of this Act, as such provisions are in effect as of the date before the enactment of this Act.

#### SEC. 13402. 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 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 13407(f)(3), not later than the date that is 60 days after the date of the enactment of this Act, 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 3002(b)(2)(B)(vi) of the Public Health Service Act,

as added by section 13101 of this Act.

(i) Report to Congress on Breaches.--

(1) In general.--Not later than 12 months after the date of the enactment of this Act 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 the date of the enactment of this title. 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.

#### SEC. 13403. EDUCATION ON HEALTH INFORMATION PRIVACY.

(a) Regional Office Privacy Advisors.--Not later than 6 months after the date of the enactment of this Act, 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 the date of the enactment of this Act, 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.

#### SEC. 13404. 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 subtitle 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.

SEC. 13405. 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 the date of the enactment of this section, 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. In issuing such guidance the Secretary shall take into consideration the guidance under section 13424(c) 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 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 section 3002(b) (2) (B) (iv) of the Public Health Service Act, as added by section 13101. 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 a 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 than 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 the date of enactment of this title, 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; and

(2) 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).

SEC. 13406. 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.

SEC. 13407. 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 13424(b)(1)(A), 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), or (iv) of section 13424(b)(1)(A) 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 13402 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 18(a) (1) (B) of the Federal Trade Commission Act (15 U.S.C. 57a(a) (1) (B)) 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 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), 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 13402(h) (2).

(B) Exception in case timely guidance not issued.--In the case that the Secretary does not issue guidance under section 13402(h) (2) 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 the date of the enactment of this section. 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.

SEC. 13408. 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 subtitle and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of the date of enactment of this title.

SEC. 13409. CLARIFICATION OF APPLICATION OF WRONGFUL DISCLOSURES CRIMINAL PENALTIES.

Section 1177(a) of the Social Security Act (42 U.S.C. 1320d-6(a)) is amended by adding at the end the following new sentence: ``For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation described in section 1180(b)(3)) and the individual obtained or disclosed such information without authorization.''

SEC. 13410. IMPROVED ENFORCEMENT.

(a) In General.--

(1) Noncompliance due to willful neglect.--Section 1176 of the Social Security Act (42 U.S.C. 1320d-5) is amended--

(A) in subsection (b)(1), by striking ``the act constitutes an offense punishable under section 1177'' and inserting ``a penalty has been imposed under section 1177 with respect to such act''; and

(B) by adding at the end the following new subsection:

``(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.').

(2) Enforcement under social security act.--Any violation by a covered entity under this subtitle is subject to enforcement and penalties under section 1176 and 1177 of the Social Security Act.

(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 the date of the enactment of this title.

(2) Not later than 18 months after the date of the enactment of this title, 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 subtitle 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 subtitle and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of the date of enactment of this Act.

(2) GAO report.--Not later than 18 months after the date of the enactment of this title, 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 the date of the enactment of this title, 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) In general.--Section 1176(a) (1) of the Social Security Act (42 U.S.C. 1320d-5(a) (1)) is amended by striking "who

violates a provision of this part a penalty of not more than'' and all that follows and inserting the following:

``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), 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) Tiers of penalties described.--Section 1176(a) of such Act (42 U.S.C. 1320d-5(a)) is further amended by adding at the end the following new paragraph:

``(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.''.

(3) Conforming amendments.--Section 1176(b) of such Act (42

U.S.C. 1320d-5(b)) is amended--

(A) by striking paragraph (2) and redesignating paragraphs (3) and (4) as paragraphs (2) and (3), respectively; and

(B) in paragraph (2), as so redesignated--

(i) in subparagraph (A), by striking ``in subparagraph (B), a penalty may not be imposed under subsection (a) if'' and all that follows through ``the failure to comply is corrected'' and inserting ``in subparagraph (B) or subsection (a) (1) (C), a penalty may not be imposed under subsection (a) if the failure to comply is corrected''; and

(ii) in subparagraph (B), by striking ``(A) (ii)'' and inserting ``(A)'' each place it appears.

(4) Effective date.--The amendments made by this subsection shall apply to violations occurring after the date of the enactment of this title.

(e) Enforcement Through State Attorneys General.--

(1) In general.--Section 1176 of the Social Security Act (42 U.S.C. 1320d-5) is amended by adding at the end the following new subsection:

``(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 1180(b) (3)) 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, United States Code.

``(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 1128A(c)(1).''.

(2) Conforming amendments.--Subsection (b) of such section, as amended by subsection (d)(3), is amended--

(A) in paragraph (1), by striking ``A penalty may not be imposed under subsection (a)'' and inserting ``No penalty may be imposed under subsection (a) and no damages obtained under subsection (d)'';

(B) in paragraph (2)(A)--

(i) after ``subsection (a)(1)(C),'', by striking ``a penalty may not be imposed under subsection (a)'' and inserting ``no penalty may be imposed under subsection (a) and no damages obtained under subsection (d)''; and

(ii) in clause (ii), by inserting ``or damages'' after ``the penalty'';

(C) in paragraph (2)(B)(i), by striking ``The period'' and inserting ``With respect to the imposition of a penalty by the Secretary under subsection (a), the period''; and

(D) in paragraph (3), by inserting ``and any damages under subsection (d)'' after ``any penalty under subsection (a)''.

(3) Effective date.--The amendments made by this subsection shall apply to violations occurring after the date of the enactment of this Act.

(f) Allowing Continued Use of Corrective Action.--Such

section is further amended by adding at the end the following new subsection:

((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.').

#### SEC. 13411. AUDITS.

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

### PART 2--RELATIONSHIP TO OTHER LAWS; REGULATORY REFERENCES; EFFECTIVE DATE; REPORTS

#### SEC. 13421. 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 subtitle in the same manner that such section applies to a provision or requirement under part C of title XI of such Act or a standard or implementation specification adopted or established under sections 1172 through 1174 of such Act.

(b) Health Insurance Portability and Accountability Act.--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 subtitle. The Secretary shall by rule amend such Federal regulations as required to make such regulations consistent with this subtitle.

(c) Construction.--Nothing in this subtitle shall constitute a waiver of any privilege otherwise applicable to an individual with respect to the protected health information of such individual.

#### SEC. 13422. REGULATORY REFERENCES.

Each reference in this subtitle to a provision of the Code of Federal Regulations refers to such provision as in effect on the date of the enactment of this title (or to the most recent update of such provision).

#### SEC. 13423. EFFECTIVE DATE.

Except as otherwise specifically provided, the provisions of part I shall take effect on the date that is 12 months after the date of the enactment of this title.

SEC. 13424. STUDIES, REPORTS, GUIDANCE.

(a) Report on Compliance.--

(1) In general.--For the first year beginning after the date of the enactment of this Act 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 subtitle 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 the date of enactment of this Act) 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 13411.

(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 the date of the enactment of this title, 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 the date of the enactment of this title, 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 the date of the enactment of this title, 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 the date of the enactment of this title, 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 the date

of enactment of this section, 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.