ROBERT GELLMAN
Privacy and Information Policy Consultant **202-543-7923**
419 Fifth Street SE **bob@bobgellman.com**
Washington, DC 20003 **www.bobgellman.com**

AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009

Excerpts from Conference Report (House Report 111-16)

Text of Law Relating to Privacy and HIPAA, followed by Conference Committee Explanation (on page 24)

*

155 Congressional Record February 12, 2009 Page H1307

TITLE XIII--HEALTH INFORMATION TECHNOLOGY

SEC. 1301. SHORT TITLE.

This title may be cited as the `Health Information Technology for Economic and Clinical Health Act' or the `HITECH Act'.

****

[Page: H1346]

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

[Page: H1347]

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 an 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 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

[Page: H1348]

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

[Page: H1349]

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 thus 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.

[Page: H1350]

``(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.

JOINT EXPLANATORY STATEMENT OF THE COMMITTEE OF CONFERENCE

****

[Page: H1433]

SUBTITLE D—PRIVACY Definitions. (House bill Sec. 4400; Senate bill Sec. 13400; Conference agreement Sec. 13400)

Current Law

Under the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA; P.L. 104–191), Congress set itself a three-year deadline to enact health information privacy legislation. If, as turned out to be the case, lawmakers were unable to pass such legislation before the deadline, the HHS Secretary was instructed to promulgate regulations containing standards to protect the privacy of individually identifiable health information. The HIPAA privacy rule (45 CFR Parts 160, 164) established a set of patient rights, including the right of access to one's medical information, and placed certain limitations on when and how health plans and health care providers may use and disclose such protected health information (PHI). Generally, plans and providers may use and disclose health information for the purpose of treatment, payment, and other health care operations without the individual's authorization and with few restrictions. In certain other circumstances (e.g., disclosures to family members and friends), the rule requires plans and providers to give the individual the opportunity to object to the disclosure. The rule also permits the use and disclosure of health information without the individual's permission for various specified activities (e.g., public health oversight, law enforcement) that are not directly connected to the treatment of the individual. For all uses and disclosures of health information that are not otherwise required or permitted by the rule, plans and providers must obtain a patient's written authorization.

The HIPAA privacy rule also permits health plans and health care providers—referred to as HIPAA covered entities—to share health information with their business associates who provide a wide variety of functions for them, including legal, actuarial, accounting, data aggregation, management, administrative, accreditation, and financial services. A covered entity is permitted to disclose health information to a business associate or to allow a business associate to create or receive health information on its behalf, provided the covered entity receives satisfactory assurance in the form of a written contract that the business associate will appropriately safeguard the information.

[Page: H1434]

In addition to health information privacy standards, HIPAA's Administrative Simplification provisions instructed the Secretary to issue security standards to safeguard PHI in electronic form against unauthorized access, use, and disclosure. The security rule (45 CFR Parts 160, 164) specifies a series of administrative, technical, and physical security procedures for providers and plans to use to ensure the confidentiality of electronic health information.

House Bill

The House bill defines the following key privacy and security terms, in most cases by reference to definitions in the HIPAA Administrative Simplification standards: breach, business associate, covered entity, disclose, electronic health record, electronic medical record, health care operations, health care provider, health plan, National Coordinator, payment, personal health record, protected health information, Secretary, security, state, treatment, use, and vendor of personal health records.

Senate Bill

Same provision.

Conference Agreement

The Conference report includes some technical modifications to the definitions. One set of such modifications is included in the definition of ''breach''. The Conference report includes a technical change to clarify that some inadvertent disclosures can constitute a breach under the meaning of this subtitle. The conference report clarifies the definition to stipulate that disclosures (as defined in 45 CFR 164.103) constitute a breach, except as otherwise provided under the definition. The definition provides that a disclosure where a person would not reasonably be able to retain the information disclosed is not a breach. Also not a breach is 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 provided that any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

Another set of such modifications pertains to the definition of Personal Health Records. Specifically, the report clarifies that Personal Health Records are ''managed, shared, and controlled by or primarily for the individual.'' This technical change clarifies that PHRs include the kinds of records managed by or for individuals, but does not include the kinds of records managed by or primarily for commercial enterprises, such as life insurance companies that maintain such records for their own business purposes. By extension, a life insurance company would not be considered a PHR vendor under this subtitle. A second clarification in the definition of PHR is the use of the term ''PHR individual identifiable health information'' (as defined in section 13407(0(2)). In the House and Senate bills, the term ''individually identifiable health information'' was used. Use of that term would have required that, to be considered a PHR, an electronic record would have to include information that was ''created or received by a health care provider, health plan, employer, or health care clearinghouse.'' However, there is increasing use of electronic records that contain personal health information that has not been created or received by a health care provider, health plan, employer, or health care clearinghouse. Use of the term ''individually identifiable health information'' would have thus improperly narrowed the scope of the term Personal Health Record under this subtitle.

Thus, the conference report included the broader term, PHR individual identifiable health information, so that the scope of the term Personal Health Record would properly include

electronic records of personal health information, regardless of whether they have been ‘‘created or received by a health care provider, health plan, employer, or health care clearinghouse.’’

PART I—IMPROVED PRIVACY PROVISIONS AND SECURITY PROVISIONS

Application of Security Provisions and Penalties to Business Associates of Covered Entities; Annual Guidance on Security Provisions. (House bill Sec. 4401; Senate bill Sec. 13401; Conference agreement Sec. 13401)

Current Law

The Security Rule promulgated pursuant to the Health Insurance Portability and Accountability Act (HIPAA) include three sets of safeguards: administrative, physical, and technical, required of covered entities (providers, health plans and healthcare clearinghouses). Administrative safeguards include such functions as assigning or delegating security responsibilities to employees, as well as security training requirements. Physical safeguards are intended to protect electronic systems and data from threats, environmental hazards, and unauthorized access. Technical safeguards are primarily IT functions used to protect and control access to data.

HIPAA permits business associates (those who perform business functions for covered entities) to create, receive, maintain or transmit electronic health information on behalf of that covered entity, provided the covered entity receives satisfactory assurance in the form of a written contract that the business associate will implement administrative, technical, and physical safeguards that reasonably and appropriately protect the information.

Violations cannot be enforced directly against business associates. Although providers and health plans are not liable for, or required to monitor, the actions of their business associates, if it finds out about a material breach or violation of the contract by a business associate, it must take reasonable steps to remedy the situation, and, if unsuccessful, terminate the contract. If termination is not feasible, the covered entity must notify HHS.

House Bill

The House bill would apply the HIPAA security standards and the civil and criminal penalties for violating those standards to business associates in the same manner as they apply to the providers and health plans for whom they are working. It also would require the Secretary, in consultation with stakeholders, to issue annual guidance on the most effective and appropriate technical safeguards, including the technologies that render information unusable, unreadable, or indecipherable recommended by the HIT Policy Committee, for protecting electronic health information.

Senate Bill

Same provision, but without any reference to recommended safeguard technologies standards.

Conference Agreement

The conference agreement includes language contained in the House bill.

Notification in the Case of Breach. (House bill Sec. 4402; Senate bill Sec. 13402; Conference agreement Sec. 13402)

Current Law

The Privacy and Security Rules promulgated pursuant to HIPAA does not require covered entities, providers, health plans or healthcare clearinghouses, to notify HHS orindividuals of a breach of the privacy, security,or integrity of their protected healthinformation.

House Bill

In the event of a breach of unsecured PHI that is discovered by a covered entity, the House bill would require the covered entity to notify each individual whose information has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of such breach. Exceptions to the breach notification requirement are for unintentional acquisition, access, use or disclosure of protected health information. For a breach of unsecured PHI under the control of a business associate, the business associate upon discovery of the breach would be required to notify the covered entity. Notice of the breach would have to be provided to the Secretary and prominent media outlets serving a particular area if more than 500 individuals in that area were impacted. If the breach impacted fewer than 500 individuals, the covered entity involved would have to maintain a log of such breaches and annually submit it to the Secretary.

The House bill would define unsecured PHI as information that is not secured through the use of a technology or methodology identified by the Secretary as rendering the information unusable, unreadable, and undecipherable to unauthorized individuals. The House bill would require the Secretary each year to report to appropriate committees in Congress on the number and type of breaches, actions taken in response, and recommendations made by the National Coordinator on how to reduce the number of breaches. Within 180 days of enactment, the Secretary would be required to issue interim final regulations to implement this section. The provisions in the section would apply to breaches discovered at least 30 days after the regulations were published.

Senate Bill

Same provision, but without any reference to recommended encryption standards in issuing annual guidance on securing PHI.

Conference Agreement

Similar provision to the House bill with one difference; notifications in cases of unintentional disclosures would be required unless such disclosure is to an individual authorized to access health information at the same facility.

Education on Health Information Privacy. (House bill Sec. 4403; Senate bill Sec. 13403; Conference agreement Sec. 13403)

Current Law

The Privacy Rule promulgated pursuant to HIPAA requires each covered entity to designate a privacy official for the development and implementation of its policies and procedures.

House Bill

Within six months of enactment, the House bill would require the Secretary to designate a privacy advisor in each HHS regional office to offer education and guidance to covered entities and business associates on their federal health information privacy and security rights and responsibilities. Within 12 months of enactment, OCR would be required to develop and maintain a national education program to educate the public about their privacy rights and the potential uses of their PHI.

Senate Bill

Same provision.

Conference Agreement

Same provision.

[Page: H1435]

Application of Privacy Provisions and Penalties to Business Associates of Covered Entities. (House bill Sec. 4404; Senate bill Sec. 13404; Conference agreement Sec. 13404)

Current Law

The Privacy Rule promulgated pursuant to HIPAA permits a covered entity to disclose health information to a business associate or to allow a business associate to create or receive health information on its behalf, provided the covered entity receives satisfactory assurance in the form of a written contract that the business associate will appropriately safeguard the information.

Violations cannot be enforced directly against business associates. Although covered entities are not liable for, or required to monitor, the actions of their business associates, if it finds out about a material breach or violation of the contract by a business associate, it must take reasonable steps to remedy the situation, and, if unsuccessful, terminate the contract. If termination is not feasible, the covered entity must notify HHS.

House Bill

The House bill would apply the HIPAA Privacy Rule, the additional privacy requirements, and the civil and criminal penalties for violating those standards to business associates in the same manner as they apply to the providers and health plans for whom they are working.

Senate Bill

Same provision.

Conference Agreement

Same provision.

Restrictions on Certain Disclosures and Sales of Health Information; Accounting of Certain Protected Health Information Disclosures; Access to Certain Information in Electronic Format. (House bill Sec. 4405; Senate bill Sec. 13405; Conference agreement Sec. 13405)

Current Law

The privacy rule established several individual privacy rights. First, it established a new federal legal right for individuals to see and obtain a copy of their own PHI in the form or format requested by the individual, if it is readily producible in such form or format. If not, then the information must be provided in hard copy or such form or format as agreed to by the covered entity and the individual. The covered entity can impose reasonable, cost-based fees for providing the information. Second, the rule gives individuals the right to amend or supplement their own PHI. The covered entity must act on an individual's request for amendment within 60 days of receiving the request. That deadline may be extended up to 30 days. Third, individuals have the right to request that a covered entity restrict the use and disclosure of their PHI for the purposes of treatment, payment, or health care operations. However, the covered entity is not required to agree to such a restriction unless it has entered into an agreement to restrict, in which case it must abide by the agreement. Finally, individuals have the right to an accounting of disclosures of their PHI by a covered entity during the previous six years, with certain exceptions. For example, a covered entity is not required to provide an accounting of disclosures that have been made to carry out treatment, payment, and health care operations. The privacy rule incorporates a minimum necessary standard. Whenever a covered entity uses or discloses PHI or requests such information from another covered entity, it must make reasonable efforts to limit the information to the minimum necessary to accomplish the intended purpose of the use or disclosure. There are a number of circumstances in which the minimum necessary standard does not apply; for example, disclosures to or requests by a health care provider for treatment purposes. The rule also permits the disclosure of a ''limited data set'' for certain specified purposes (e.g., research), pursuant to a data use agreement with the recipient. A limited data set, while not meeting the rule's definition of de-identified information (see below), has most direct identifiers removed and is considered by HHS to pose a low privacy risk.

House Bill

The House bill would give individuals the right to receive an electronic copy of their PHI, if it is maintained in an electronic health record. Any associated fee charged by the covered entity could only cover its labor costs for providing the electronic copy. The bill would require a health care provider to honor a patient's request that the PHI regarding a specific health care item or service not be disclosed to a health plan for purposes of payment or health care operations, if the patient paid out-of-pocket in full for that item or service. The House bill also would give an individual the right to receive an accounting of PHI disclosures made by covered entities or their business associates for treatment, payment, and health care operations during the previous three years, if the disclosures were through an electronic health record. Within 18 months of adopting standards on accounting of disclosures (as required under PHSA Section 3002, as added by Section 4101 of this Act), the Secretary would be required to issue regulations on what information shall be collected about each disclosure. For current users of electronic health records, the accounting requirements would apply to disclosures made on or after January 1, 2014. For covered entities yet to acquire electronic health records, the accounting requirements would apply to disclosures on or after January 1, 2011, or the date of electronic health record acquisition, whichever is later.

The House bill would require covered entities to limit the use, disclosure, or, request of PHI, to the extent practicable, to a limited data set or, if needed, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request. This requirement would sunset at such a time as the Secretary issues guidance on what constitutes minimum necessary. The Secretary would have 18 months to issue such guidance. In addition, the bill would clarify that the entity disclosing the PHI (as opposed to the requester) makes the minimum necessary determination. The HIPAA privacy rule's exceptions to the minimum necessary standard would continue to apply. Within 18 months of enactment, the Secretary would be required to issue regulations to eliminate from the definition of health care operations those activities that can reasonably and efficiently be conducted with deidentified information or that should require authorization for the use or disclosure of PHI.

The House bill would prohibit the sale of PHI by a covered entity or business associate without patient authorization except in certain specified circumstances, such as to recoup the costs of preparing and transmitting data for public health or research activities (as defined in the HIPAA privacy rule), or to provide an individual with a copy of his or her PHI. Within 18 months of enactment, the Secretary would be required to issue regulations governing the sale of PHI.

Finally, the House bill specifies that none of its provisions would constitute a waiver of any health privacy privilege otherwise applicable to an individual.

Senate Bill

The Senate bill includes all the same provisions as the House bill, other than the final provision protecting an individual's health privacy privileges, but with the following additional language: (1) in developing guidance on what constitutes minimum necessary, the Secretary would be required to take into consideration the information necessary to improve patient outcomes and to manage chronic disease; (2) in developing regulations on the accounting of disclosures through an EHR, the Secretary would be required to take into account an individual's interest in learning when the PHI was disclosed and to whom, as well as the cost of accounting for such disclosures;

(3) regarding the definition of health care operations, the Secretary would be required to review and evaluate the definition and, to the extent necessary, eliminate those activities that could reasonably and efficiently be conducted using deidentified information or that should require authorization; (4) the Secretary could not require the use of de-identified information or require authorization for the use and disclosure of information for activities within a covered entity that are described in paragraph one of the definition of health care operations; and (6) in developing regulation governing the sale of PHI, the Secretary would be required to evaluate the impact of charging an amount to cover the costs of preparing and transmitting data for public health or research activities.

Conference Agreement

The conference agreement maintains most of these provisions but makes small modifications. The conference agreement takes the Senate changes on issuing guidance on what constitutes minimum necessary and what factors have to be considered. The conference agreement requires an accounting of disclosures but has a longer timeframe for allowing providers to come into compliance with this requirement than the House bill and shorter than the Senate bill. The requirement to account for disclosures under this section is prospective. For example, a covered entity that acquires an electronic health record as of June 30, 2012 would be required to account for disclosures made through that electronic health record as of June 30, 2012 and forward. The covered entity would be required to retain that accounting for a period of three years. Thus, if an individual requested an accounting for disclosures on June 30, 2015, the covered entity would be required to provide that accounting for the period of June 30, 2012 to June 30, 2015, with respect to such individual, consistent with the requirements of Section 13405. However, if an individual requested an accounting of disclosures on June 30, 2013, the covered entity would be required to provide such accounting only for the period of June 30, 2012 to June 30, 2013.

Section 13405(c)(4) of the Senate-passed bill included a provision allowing the imposition of a reasonable fee for the accounting for disclosures required under this Section. However, this statutory provision was duplicative of an existing provision under 45 CFR 164.528(c)(2) which already allows for the imposition of a reasonable fee for providing such accounting, so the provision from the Senate passed bill was struck.

The conference agreement strikes the provision requiring the Secretary to review the definition of health care operations. The conference agreement permits the sale of protected health information in cases of research but only limited to costs of preparing and transmitting data. It also permits the sale of protected health information for public health activities the Secretary is required to study and determine whether costs

should be limited. The conference agreement allows an individual to request their health information in an electronic format if it is maintained in such a format for a reasonable cost based fee as it was in the House and Senate bills. The conference agreement permits the individual to designate that the information be sent to another entity or person. Finally, the conference agreement specifies that none of its provisions would constitute a waiver of any

health privacy privilege otherwise applicable to an individual, but moves this provision to section 13421 Relationship to Other Laws.

Conditions of Certain Contacts as Part of Health Care Operations. (House bill Sec. 4406; Senate bill Sec. 13406; Conference agreement Sec. 13406)

Current Law

Generally, covered entities may use and disclose health information for the purpose of treatment, payment, and other health care operations without the individual's authorization and with few restrictions. Health care operations are broadly defined to include quality assessment and improvement activities, case management and care coordination, evaluation of health care professionals, underwriting, legal services, business planning, customer services, grievance resolution, and fundraising.

Under the Privacy Rule promulgated pursuant to HIPAA, a covered entity may not disclose health information to a third party (e.g., pharmaceutical company), in exchange for direct or indirect remuneration, for the marketing activities of the third party without first obtaining a patient's authorization. Similarly, a covered entity may not use or disclose health information for its own marketing activities without authorization.

Marketing is defined as a communication about a product or service that encourages the recipient to purchase or use the product or service. However, communications made by a covered entity (or its business associate) to encourage a patient to purchase or use a health care-related product or service are excluded from this definition and, therefore, do not require the patient's authorization, even if the covered entity is paid by a third party to engage in such activities.

House Bill

The House bill would clarify that a marketing communication by a covered entity or business associate about a product or service that encourages the recipient to purchase or use the product or service may not be considered a health care operation, unless the communication relates to a health carerelated product or service. Further, it would prohibit a covered entity or business associate from receiving direct or indirect payment for marketing a health care-related product or service without first obtaining the recipient's authorization. Business associates would be permitted to receive payment from a covered entity for making any such communication on behalf of the covered entity that is consistent with the contract. Fundraising using a patient's protected health information would not be permitted without a patient's authorization.

Senate Bill

Like the House bill, the Senate bill would clarify that a marketing communication by a covered entity or business associate about a product or service that encourages the recipient to purchase or use the product or service may not be considered a health care operation, unless the communication relates to a health care-related product or service. Further, the Senate bill states that a communication about a health care-related product or service would be permitted as a

healthcare operation including where the covered entity receives payment for making the communications where (1) the communication only describes a health care item or service previously prescribed for or administered to the recipient, or (2) the covered entity or business associate obtains authorization. Finally, the Senate bill does not include the House provision on fundraising.

Conference Agreement

The conference agreement retains the general rules about marketing in both the House and Senate bills. The conference report makes an exception and allows providers to be paid reasonable fees as determined by the Secretary to make a communication to their patients about a drug or biologic that the patient is currently prescribed. The conference agreement continues to permit fundraising activities by the provider using a patient's protected health information so long as any written fundraising provide an opportunity to opt out of future fundraising communications. If the recipient chooses to opt out of future fundraising communications, that choice is treated as a revocation of authorization under 45 CFR 164.508. All the protections that apply under 45 CFR 164.508 to an individual who has revoked an authorization would thus apply to a recipient of communications who chooses to opt out of receiving future fundraising communications, including the right not to be denied treatment as a result of making that choice.

Temporary Breach Notification Requirement for Vendors of Personal Health Records and Other Non-HIPAA Covered Entities. (House bill Sec. 4407; Senate bill Sec. 13407; Conference agreement Sec. 13407)

Current Law

There is no Federal law that requires entities to notify individual when their health information has been breached.

House Bill

The House bill would require personal health record (PHR) vendors and entities offering products and services through a PHR vendor's website, upon discovery of a breach of security of unsecured PHR health information, to notify the individuals impacted and the FTC. Further, third party service providers that provide services to PHR vendors and to other entities offering products and services through a PHR vendor's website and, as a result, that handle unsecured PHR health information would, following the discovery of a breach of security of such information, be required to notify the vendor or other entity. The requirements in Section 4402 for the content and timeliness of notifications also would apply to this section. Unsecured PHR health information means PHR health information that is not protected through the use of a technology or methodology specified by the Secretary in guidance issued pursuant to Section 4402.

The FTC would be required to notify HHS of any breach notices it received and would given enforcement authority regarding such breaches of unsecured PHR health information. Within 180 days, the Secretary would be required to issue interim final regulations to implement this

section. The provisions in the section would apply to breaches discovered no sooner than 30 days after the regulations are published. The provisions in this section would no longer apply to breaches occurring after HHS or FTC had adopted new privacy and security standards for non-HIPAA covered entities, including requirements relating to breach notification.

Senate Bill

The Senate bill includes the same provisions.

Conference Agreement

The conference agreement is the same as the House and Senate language with minor clarifications. The conference agreement requires the FTC issue regulations as opposed to the Secretary of HHS. The conference agreement applies the breach notification provision to entities that access and receive health information to and from a personal health record.

Business Associate Contracts Required for Certain Entities. (House bill Sec. 4408; Senate bill Sec. 13408; Conference agreement Sec. 13408)

Current Law

A covered entity (a provider, health plan, of clearinghouse) is permitted to disclose health information to a business associate or to allow a business associate to create or receive health information on its behalf, provided the covered entity receives satisfactory assurance in the form of a written contract that the business associate will appropriately safeguard the information. Current law does not explicitly include or exclude regional health information exchanges, regional health information organizations, and others offering personal health records for a covered entity from regulation under the Privacy Rule promulgated under HIPAA.

House Bill

The House bill requires organizations that contract with covered entities for the purpose of exchanging electronic health information, for example, Health Information Exchanges, Regional Health Information Organizations (RHIOs), and PHR vendors that offer their products through or for a provider or health plan, to have business associate contracts with those providers or health plans.

Senate Bill

Same provision.

Conference Agreement

Same provision.

Clarification of Application of Wrongful Disclosures Criminal Penalties. (House bill Sec. 4409; Senate bill Sec. 13409; Conference agreement Sec. 13409)

Current Law

The HIPAA criminal penalties include fines of up to $250,000 and up to 10 years in prison for disclosing or obtaining health information with the intent to sell, transfer or use it for commercial advantage, personal gain, or malicious harm. In July 2005, the Justice Department Office of Legal Counsel (OLC) addressed which persons may be prosecuted under HIPAA and concluded that only a covered entity could be criminally liable.

House Bill

The House bill clarifies that criminal penalties for wrongful disclosure of PHI apply to individuals who without authorization obtain or disclose such information maintained by a covered entity, whether they are employees or not.

Senate Bill

Same provision.

Conference Agreement

Same provision.

Improved Enforcement. (House bill Sec. 4410; Senate bill Sec. 13410; Conference agreement Sec. 13410)

Current Law

HIPAA authorized the Secretary to impose civil monetary penalties on any person failing to comply with the privacy and security standards. The maximum civil fine is $100 per violation and up to $25,000 for all violations of an identical requirement or prohibition during a calendar year. Civil monetary penalties may not be imposed if (1) the violation is a criminal offense under HIPAA's criminal penalty provisions (see below); (2) the person did not have actual or constructive knowledge of the violation; or (3) the

failure to comply was due to reasonable cause and not to willful neglect, and the failure to comply was corrected during a 30-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred. For certain wrongful disclosures of PHI, OCR may refer the case to the Department of Justice for criminal prosecution. HIPAA's criminal penalties include fines of up to $250,000 and up to 10 years in prison for disclosing or obtaining health information with the intent to sell, transfer or use it for commercial advantage, personal gain, or malicious harm.

House Bill

The House bill would amend HIPAA to permit OCR to pursue an investigation and the imposition of civil monetary penalties against any individual for an alleged criminal violation of the Privacy and Security Rule of HIPAA if the Justice Department had not prosecuted the individual. In addition, the bill would amend HIPAA to require a formal investigation of complaints and the imposition of civil monetary penalties for violations due to willful neglect. The Secretary would be required to issue regulations within 18 months to implement those amendments. The bill also would require that any civil monetary penalties collected be transferred to OCR to be used for enforcing the HIPAA privacy and security standards. Within 18 months of enactment, GAO would be required to submit recommendations for giving a percentage of any civil monetary penalties collected to the individuals harmed. Based on those recommendations, the Secretary, within three years of enactment, would be required to establish by regulation a methodology to distribute a percentage of any collected penalties to harmed individuals.

The House bill would increase and tier the penalties for violations of HIPAA. It would preserve the current requirement that a civil fine not be imposed if the violation was due to reasonable cause and was corrected within 30 days.

Finally, the House bill would authorize State Attorneys General to bring a civil action in Federal district court against individuals who violate the HIPAA privacy and security standards, in order to enjoin further such violation and seek damages of up to $100 per violation, capped at $25,000 for all violations of an identical requirement or prohibition in any calendar year. State action against a person would not be permitted if a federal civil action against that same individual was pending. Nothing in this section would prevent OCR from continuing to use corrective action without a penalty in cases where the person did not know, and by exercising reasonable diligence would not have known, about the violation.

Senate Bill

Same provision.

Conference Agreement

Same provision.

Audits. (House bill Sec. 4411; Senate bill Sec. 13411; Conference agreement Sec. 13411)

Current Law

The Secretary is authorized to conduct compliance reviews to determine whether covered entities are complying with HIPAA standards.

House Bill

The House bill would require the Secretary to perform periodic audits to ensure compliance with the Privacy and Security Rule promulgated pursuant to HIPAA and the requirements of this subtitle.

Senate Bill

Same provision.

Conference Agreement

Same provision.

Special Rule for Information to Reduce Medication Errors and Improve Patient Safety. (House bill Sec. 4412)

Current Law Under the privacy rule, communications made by a covered entity (or its business associate) to encourage a patient to purchase or use a health care-related product or service are excluded from the definition of marketing and, therefore, do not require the patient's authorization, even if the covered entity is paid by a third party to engage in such activities.

House Bill

The House bill states that none of the privacy provisions in the bill would prevent a pharmacist from communicating with patients to reduce medication errors and improve patient safety provided there is no remuneration other than for treatment of the individual and payment for such treatment. The Secretary would be permitted by regulation to allow pharmacists to receive reasonable, cost-based payment for such communications, if it is determined that this would improve patient care and protect PHI.

Senate Bill

Tile Senate bill does not include this same provision, but has corresponding limitation in section 13406 of the Senate bill.

Conference Agreement

The conference agreement does not include this same provision, but has corresponding limitations in section 13406.

PART H—RELATIONSHIP TO OTHER LAWS; REGULATORY REFERENCES; EFFECTIVE DATE; REPORTS

Relationship to Other Laws. (House bill Sec. 4421; Senate bill Sec. 13421; Conference agreement Sec. 13421)

Current Law

Under Section 1178 of the Social Security Act, as amended by HIPAA, the security standards preempt any contrary provision of state law, with certain specified exceptions (e.g., public health reporting). Pursuant to HIPAA Section 264, however, the privacy rule does not preempt a contrary provision of state law that is more protective of patient medical privacy. Psychotherapy notes (i.e., notes recorded by a mental health professional during counseling) are afforded special protection under the privacy rule. Almost all uses and disclosures of such information require patient authorization.

House Bill

The House bill would apply the preemption provisions in SSA Section 1178 to the requirements of this subtitle and preserve the HIPAA privacy and security standards to the extent that they are consistent with the subtitle. The Secretary would be required by rulemaking to amend such standards as necessary to make them consistent with this subtitle.

Senate Bill

The Senate bill includes the same provisions; with the additional requirement that the Secretary revise the definition of psychotherapy notes to include test data that are part of a mental health evaluation.

Conference Agreement

The conference agreement takes language from the House bill. The provision related to psychotherapy notes is moved in the conference report.

Regulatory References. (House bill Sec. 4422; Senate bill Sec. 13422; Conference agreement Sec. 13422)

Current Law

No provision.

House Bill

The House bill states that each reference in this subtitle to a federal regulation refers to the most recent version of the regulation.

Senate Bill

Same provision.

Conference Agreement

Same provision.

Effective Date. (House bill Sec. 4423; Senate bill Sec. 13423; Conference agreement Sec. 13423)

Current Law

No provision.

House Bill

Except as otherwise specifically provided, the provisions in this subtitle would become effective 12 months after enactment.

Senate Bill

Same provision.

Conference Agreement

Same provision.

Studies, Reports, Guidance. (House bill Sec. 4424; Senate bill Sec. 13424; Conference agreement Sec. 13424)

Current Law

Any person who believes a covered entity is not complying with the privacy rule may file a complaint with HHS. The rule authorizes the Secretary to conduct investigations to determine whether covered entities are in compliance. HIPAA does not require the Secretary to issue a compliance report.

The HIPAA Administrative Simplification standards apply to individual and group health plans that provide or pay for medical care; health care clearinghouses (i.e., entities that facilitate and process the flow of information between health care providers and payers); and health care providers. In addition, the privacy and security standards apply to business associates with whom covered entities share health information. They do not apply directly to other entities that collect and maintain health information, including Health Information Exchanges, RHIOs, and PHR vendors, unless they are acting as providers or plans.

The HIPAA standards are intended to protect individually identifiable health information; de-identified information is not subject to the regulations. Under the privacy rule, health information is de-identified if 18 specific identifiers (e.g., name, social security number, address) have been removed, or if a qualified statistician, using accepted principles, determines that the risk if very small that the individual could be identified. Generally, plans and providers may use and disclose health information for the purpose of treatment, payment, and other health care operations without the individual's authorization and with few restrictions. Covered entities may, but are

not required, to obtain an individual's general consent to use or disclose PHI for treatment, payment, or health care operations.

House Bill

The Secretary would be required annually to submit to specified Congressional Committees and post online a compliance report containing information on (1) the number and nature of complaints of alleged violations and how they were resolved, including the imposition of civil fines, (2) the number of covered entities receiving technical assistance in order to achieve compliance, as well as the types of assistance provided, (3) the number of audits performed and a summary of their findings, and (4) the Secretary's plan for the following year for improving compliance with and enforcement of the HIPAA standards and the provisions of this subtitle. The House bill would require the Secretary, within one year and in consultation

[Page: H1438]

with the Federal Trade Commission (FTC), to study the application of health information privacy and security requirements (including breach notification) to non-HIPAA covered entities and report the findings to specified House (Ways and Means, Energy and Commerce) and Senate (Finance, HELP) Committees. The report should include an examination of PHR vendors and other entities that offer products and services through the websites of PHR vendors and covered entities, provide a determination of which federal agency is best equipped to enforce new requirements for non-HIPAA covered entities, and include a time frame for implementing regulations.

The House bill would require the Secretary, within one year of enactment and in consultation with stakeholders, to issue guidance on how best to implement the HIPAA privacy rule's requirements for deidentifying PHI.

The House bill would require GAO, within one year, to report to the House Ways and Means and Energy and Commerce Committees and the Senate Finance Committee on best practices related to the disclosure of PHI among health care providers for the purpose of treatment. The report must include an examination of practices implemented by states and other entities, such as health information exchanges, and how those practices improve the quality of care, as well as an examination of the use of electronic informed consent for disclosing PHI for treatment, payment, and health care operations.

Senate Bill

The Senate bill includes the same provisions, with the additional requirement that GAO, within one year, report to Congress and the Secretary on the impact of the bill's privacy provisions on health care costs.

Conference Agreement

The conference agreement maintains most all study language and add a study to requires the Secretary to review the definition of ''psychotherapy notes'' with regard to including test data

that are part of a mental health evaluation. The Secretary may revise the definition by regulation based on the recommendations of the study. In addition, the conference agreement broadened the study added by the Senate on the impact of the bill's privacy provisions on health care costs. It requires the GAO to study all impact of all the provisions of the HITECH Act on health care costs, adoption of electronic health record by providers, and reductions in medical errors and other quality improvements.

****