PUBLIC LAW 111–5—FEB. 17, 2009
Division A, Title XIII, Subtitle D

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. 57*a*(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.

Division A, Title XIII, Subtitle D

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.