

sociates that are subject to the requirements of this subchapter and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of February 17, 2009, comply with such requirements.

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

Editorial Notes

REFERENCES IN TEXT

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

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

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

§ 17941. Recognition of security practices

(a) In general

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

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

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

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

(b) Definition and miscellaneous provisions

(1) Recognized security practices

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

(2) Limitation

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

(3) No liability for nonparticipation

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

(4) Rule of construction

Nothing in this section shall be construed to limit the Secretary’s authority to enforce the HIPAA Security rule (part 160 of title 45 Code of Federal Regulations and subparts A and C of part 164 of such title), or to supersede or conflict with an entity or business associate’s obligations under the HIPAA Security rule.

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

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

§ 17951. Relationship to other laws

(a) Application of HIPAA State preemption

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

(b) Health Insurance Portability and Accountability Act of 1996

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

(c) Construction

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

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

Editorial Notes

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original “this subtitle”, meaning subtitle D (§13400 et seq.) of title XIII of div. A of Pub. L. 111-5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this sub-

chapter. For complete classification of subtitle D to the Code, see Tables.

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

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

§ 17952. Regulatory references

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

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

Editorial Notes

REFERENCES IN TEXT

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

§ 17953. Studies, reports, guidance

(a) Report on compliance

(1) In general

For the first year beginning after February 17, 2009, and annually thereafter, the Secretary shall prepare and submit to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Ways and Means and the Committee on Energy and Commerce of the House of Representatives a report concerning complaints of alleged violations of law, including the provisions of this subchapter as well as the provisions of subparts C and E of part 164 of title 45, Code of Federal Regulations, (as such provisions are in effect as of February 17, 2009) relating to privacy and security of health information that are received by the Secretary during the year for which the report is being prepared. Each such report shall include, with respect to such complaints received during the year—

(A) the number of such complaints;

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

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

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

(E) the number of subpoenas or inquiries issued;

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

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

(2) Availability to public

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

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

(1) Study

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

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

(i) vendors of personal health records;

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

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

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

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

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

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

(2) Report

The Secretary shall submit to the Committee on Finance, the Committee on Health, Education, Labor, and Pensions, and the Committee on Commerce of the Senate and the