

PART A—IMPROVED PRIVACY PROVISIONS AND SECURITY PROVISIONS

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

Sections 164.308, 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity. The additional requirements of this title¹ that relate to security and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.

(b) Application of civil and criminal penalties

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

(c) Annual guidance

For the first year beginning after February 17, 2009, and annually thereafter, the Secretary of Health and Human Services shall, after consultation with stakeholders, annually issue guidance on the most effective and appropriate technical safeguards for use in carrying out the sections referred to in subsection (a) and the security standards in subpart C of part 164 of title 45, Code of Federal Regulations, including the use of standards developed under section 300jj-12(b)(2)(B)(vi) of this title, as added by section 13101 of this Act, as such provisions are in effect as of the date before February 17, 2009.²

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

REFERENCES IN TEXT

This title, referred to in subsec. (a), is title XIII of div. A of Pub. L. 111-5, which enacted this chapter and subchapter XXVIII (§300jj et seq.) of chapter 6A this title, amended sections 1320d, 1320d-5, and 1320d-6 of this title, and enacted provisions set out as a note under this section and section 201 of this title. For complete classification of title XIII to the Code, see Short Title of 2009 Amendment note set out under section 201 of this title and Tables.

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

EFFECTIVE DATE

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

¹ See References in Text note below.

² So in original. Section 300jj-12 of this title was enacted on Feb. 17, 2009.

§ 17932. Notification in the case of breach**(a) In general**

A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.

(b) Notification of covered entity by business associate

A business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach.

(c) Breaches treated as discovered

For purposes of this section, a breach shall be treated as discovered by a covered entity or by a business associate as of the first day on which such breach is known to such entity or associate, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such entity or associate, respectively) or should reasonably have been known to such entity or associate (or person) to have occurred.

(d) Timeliness of notification**(1) In general**

Subject to subsection (g), all notifications required under this section shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by the covered entity involved (or business associate involved in the case of a notification required under subsection (b)).

(2) Burden of proof

The covered entity involved (or business associate involved in the case of a notification required under subsection (b)), shall have the burden of demonstrating that all notifications were made as required under this part, including evidence demonstrating the necessity of any delay.

(e) Methods of notice**(1) Individual notice**

Notice required under this section to be provided to an individual, with respect to a breach, shall be provided promptly and in the following form:

(A) Written notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or, if specified