

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 1320d-9(b)(3) of this title) and the individual obtained or disclosed such information without authorization.

**(b) Penalties**

A person described in subsection (a) shall—

(1) be fined not more than \$50,000, imprisoned not more than 1 year, or both;

(2) if the offense is committed under false pretenses, be fined not more than \$100,000, imprisoned not more than 5 years, or both; and

(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than \$250,000, imprisoned not more than 10 years, or both.

(Aug. 14, 1935, ch. 531, title XI, §1177, as added Pub. L. 104-191, title II, §262(a), Aug. 21, 1996, 110 Stat. 2029; amended Pub. L. 111-5, div. A, title XIII, §13409, Feb. 17, 2009, 123 Stat. 271.)

AMENDMENTS

2009—Subsec. (a). Pub. L. 111-5 inserted at end “For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation described in section 1320d-9(b)(3) of this title) and the individual obtained or disclosed such information without authorization.”

EFFECTIVE DATE OF 2009 AMENDMENT

Amendment by Pub. L. 111-5 effective 12 months after Feb. 17, 2009, see section 13423 of Pub. L. 111-5, set out as an Effective Date note under section 17931 of this title.

**§ 1320d-7. Effect on State law**

**(a) General effect**

**(1) General rule**

Except as provided in paragraph (2), a provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1320d-1 through 1320d-3 of this title, shall supersede any contrary provision of State law, including a provision of State law that requires medical or health plan records (including billing information) to be maintained or transmitted in written rather than electronic form.

**(2) Exceptions**

A provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1320d-1 through 1320d-3 of this title, shall not supersede a contrary provision of State law, if the provision of State law—

(A) is a provision the Secretary determines—

(i) is necessary—

(I) to prevent fraud and abuse;

(II) to ensure appropriate State regulation of insurance and health plans;

(III) for State reporting on health care delivery or costs; or

(IV) for other purposes; or

(ii) addresses controlled substances; or

(B) subject to section 264(c)(2) of the Health Insurance Portability and Accountability Act of 1996, relates to the privacy of individually identifiable health information.

**(b) Public health**

Nothing in this part shall be construed to invalidate or limit the authority, power, or procedures established under any law providing for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention.

**(c) State regulatory reporting**

Nothing in this part shall limit the ability of a State to require a health plan to report, or to provide access to, information for management audits, financial audits, program monitoring and evaluation, facility licensure or certification, or individual licensure or certification.

(Aug. 14, 1935, ch. 531, title XI, §1178, as added Pub. L. 104-191, title II, §262(a), Aug. 21, 1996, 110 Stat. 2029.)

REFERENCES IN TEXT

Section 264(c)(2) of the Health Insurance Portability and Accountability Act of 1996, referred to in subsec. (a)(2)(B), is section 264(c)(2) of Pub. L. 104-191, which is set out as a note under section 1320d-2 of this title.

**§ 1320d-8. Processing payment transactions by financial institutions**

To the extent that an entity is engaged in activities of a financial institution (as defined in section 3401 of title 12), or is engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments, for a financial institution, this part, and any standard adopted under this part, shall not apply to the entity with respect to such activities, including the following:

(1) The use or disclosure of information by the entity for authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting, a payment for, or related to, health plan premiums or health care, where such payment is made by any means, including a credit, debit, or other payment card, an account, check, or electronic funds transfer.

(2) The request for, or the use or disclosure of, information by the entity with respect to a payment described in paragraph (1)—

(A) for transferring receivables;

(B) for auditing;

(C) in connection with—

(i) a customer dispute; or

(ii) an inquiry from, or to, a customer;

(D) in a communication to a customer of the entity regarding the customer's transactions, payment card, account, check, or electronic funds transfer;

(E) for reporting to consumer reporting agencies; or

(F) for complying with—

(i) a civil or criminal subpoena; or

(ii) a Federal or State law regulating the entity.

(Aug. 14, 1935, ch. 531, title XI, §1179, as added Pub. L. 104-191, title II, §262(a), Aug. 21, 1996, 110 Stat. 2030.)