H. R. 7898

One Hundred Sixteenth Congress of the United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Friday, the third day of January, two thousand and twenty

An Act

To amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. RECOGNITION OF SECURITY PRACTICES.

Part 1 of subtitle D of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.) is amended by adding at the end the following:

"SEC. 13412. RECOGNITION OF SECURITY PRACTICES.

"(a) IN GENERAL.—Consistent with the authority of the Secretary under sections 1176 and 1177 of the Social Security Act, when making determinations relating to fines under such section 1176 (as amended by section 13410) or such section 1177, decreasing the length and extent of an audit under section 13411, 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 1176 of the Social Security Act (as amended by section 13410);

"(2) result in the early, favorable termination of an audit under section 13411; 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 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, 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 1176 of the Social Security Act (as amended by section 13410), or the length, extent or quantity of audits under section 13411, 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.".

SEC. 2. TECHNICAL CORRECTION.

(a) IN GENERAL.—Section 3022(b) of the Public Health Service Act (42 U.S.C. 300jj–52(b)) is amended by adding at the end the following new paragraph:

"(4) APPLICATION OF AUTHORITIES UNDER INSPECTOR GENERAL ACT OF 1978.—In carrying out this subsection, the Inspector General shall have the same authorities as provided under section 6 of the Inspector General Act of 1978 (5 U.S.C. App.).".

(b) EFFECTIVE DATE.—The amendment made by subsection (a) shall take effect as if included in the enactment of the 21st Century Cures Act (Public Law 114–255).

Speaker of the House of Representatives.

Vice President of the United States and
President of the Senate.