

116TH CONGRESS
1ST SESSION

H. R. 5386

To amend the Health Information Technology for Economic and Clinical Health Act to require consideration, in certain circumstances, of whether a covered entity or business associate has adequately demonstrated that it had recognized security practices, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

DECEMBER 10, 2019

Mr. MCNERNEY (for himself and Mr. BUCSHON) introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committee on Ways and Means, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To amend the Health Information Technology for Economic and Clinical Health Act to require consideration, in certain circumstances, of whether a covered entity or business associate has adequately demonstrated that it had recognized security practices, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Promoting Better Pa-
5 tient Data Security Act of 2019”.

1 **SEC. 2. RECOGNITION OF SECURITY PRACTICES.**

2 Part 1 of subtitle D of the Health Information Tech-
3 nology for Economic and Clinical Health Act (42 U.S.C.
4 17931 et seq.) is amended by adding at the end the fol-
5 lowing:

6 **“SEC. 13412. RECOGNITION OF SECURITY PRACTICES.**

7 “(a) IN GENERAL.—Consistent with the authority of
8 the Secretary under sections 1176 and 1177 of the Social
9 Security Act, when making determinations relating to
10 fines under section 13410, decreasing the length and ex-
11 tent of an audit under section 13411, or remedies other-
12 wise agreed to by the Secretary, the Secretary shall con-
13 sider whether the covered entity or business associate has
14 adequately demonstrated that it had, for not less than the
15 previous 12 months, recognized security practices in place
16 that may—

17 “(1) mitigate fines under section 13410;

18 “(2) result in the early, favorable termination
19 of an audit under section 13411; and

20 “(3) mitigate the remedies that would otherwise
21 be agreed to in any agreement with respect to re-
22 solving potential violations of the HIPAA Security
23 rule (part 160 of title 45 Code of Federal Regula-
24 tions and subparts A and C of part 164 of such
25 title) between the covered entity or business asso-

1 ciate and the Department of Health and Human
2 Services.

3 “(b) DEFINITION AND MISCELLANEOUS PROVI-
4 SIONS.—

5 “(1) RECOGNIZED SECURITY PRACTICES.—The
6 term ‘recognized security practices’ means the stand-
7 ards, guidelines, best practices, methodologies, pro-
8 cedures, and processes developed under section
9 2(c)(15) of the National Institute of Standards and
10 Technology Act, the approaches promulgated under
11 section 405(d) of the Cybersecurity Act of 2015, and
12 other programs and processes that address cyberse-
13 curity and that are developed, recognized, or promul-
14 gated through regulations under other statutory au-
15 thorities. Such practices shall be determined by the
16 covered entity or business associate.

17 “(2) LIMITATION.—Nothing in this section
18 shall be construed as providing the Secretary author-
19 ity to increase fines under section 13410, or the
20 length, extent or quantity of audits under section
21 13411, due to a lack of compliance with the recog-
22 nized security practices.

23 “(3) NO LIABILITY FOR NONPARTICIPATION.—
24 Subject to paragraph (4), nothing in this section
25 shall be construed to subject a covered entity or

1 business associate to liability for electing not to en-
2 gage in the recognized security practices defined by
3 this section.

4 “(4) RULE OF CONSTRUCTION.—Nothing in
5 this section shall be construed to limit the Sec-
6 retary’s authority to enforce the HIPAA Security
7 rule (part 160 of title 45 Code of Federal Regula-
8 tions and subparts A and C of part 164 of such
9 title), or to supersede or conflict with an entity or
10 business associate’s obligations under the HIPAA
11 Security rule.”.

○