116TH CONGRESS
1ST SESSION

S. 1842

To protect the personal health data of all Americans.

IN THE SENATE OF THE UNITED STATES

JUNE 13, 2019

Ms. KLOBUCHAR (for herself and Ms. MURKOWSKI) introduced the following bill; which was read twice and referred to the Committee on Health, Education, Labor, and Pensions

---

A BILL

To protect the personal health data of all Americans.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Protecting Personal Health Data Act''.

SEC. 2. FINDINGS.

Congress finds as follows:

(1) On July 19, 2016, the Department of Health and Human Services, acting through the Office of the National Coordinator for Health Information Technology and in coordination with the Office

for Civil Rights of the Department of Health and Human Services and the Federal Trade Commission, issued a report to Congress entitled ''Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA'' (referred to in this section as the ''report'') about the need to enact modern protections for consumers' personal health data.

(2) The report states that ''[t]he wearable fitness trackers, social media sites where individuals share health information through specific social networks, and other technologies that are common today did not exist when Congress enacted the Health Insurance Portability and Accountability Act of 1996''.

(3) The report states that entities not covered by the privacy protections of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191), such as wearable fitness trackers and health-focused social media sites, ''engage in a variety of practices such as online advertising and marketing, commercial uses or sale of individual information, and behavioral tracking practices, all of which indicate information use that is likely broader than what individuals would anticipate''.

(4) The report ''identifies key gaps that exist between HIPAA regulated entities and those not regulated by HIPAA'' and ''recommends addressing those gaps in a way that protects consumers while leveling the playing field for innovators inside and outside of HIPAA''.

SEC. 3. DEFINITIONS.

In this Act:

(1) CONSUMER DEVICES, SERVICES, APPLICATIONS, AND SOFTWARE.—

(A) IN GENERAL.—Except as provided in subparagraph (C), the term ''consumer devices, services, applications, and software'' means devices, services, applications, and software—

(i) that are primarily designed for or marketed to consumers; and

(ii) a substantial purpose or use of which is to collect or use personal health data.

(B) INCLUSION.—The term ''consumer devices, services, applications, and software'' shall include, but is not limited to—

(i) direct-to-consumer genetic testing services;

(ii) cloud-based or mobile technologies that are designed to collect individuals' personal health data directly or indirectly with individuals' consent, which could enable sharing of such information, such as wearable fitness trackers; and

(iii) internet-based social media sites which are primarily designed for, or marketed to, consumers to collect or use personal health data, including sites that share health conditions and experiences.

(C) EXCEPTION.—The term ''consumer devices, services, applications, and software'' shall not include—

(i) products on which personal health data is derived solely from other information that is not personal health data, such as Global Positioning System data; or

(ii) products primarily designed for, or marketed to, covered entities and business associates (as defined for purposes of regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note)).

(2) DIRECT-TO-CONSUMER GENETIC TESTING SERVICES.—The term ''direct-to-consumer genetic testing service'' means a service, which may include a test that analyzes various aspects of an individual's genetic material, that enables a consumer to have access to their genetic information, or to information derived therefrom, without the need to have a health care provider or health insurance issuer participate in the process of gaining access.

(3) NATIONAL COORDINATOR.—The term ''National Coordinator'' means the National Coordinator for Health Information Technology at the Department of Health and Human Services.

(4) OPERATOR.—The term ''operator'' means any person who operates any type of consumer devices, services, applications, and software or who provides consumer devices, services, applications, and software for the use of consumers and collects or maintains personal health data from or about the users of such consumer devices, services, applications, and software.

(5) PERSONAL HEALTH DATA.—The term ''personal health data'' means any information, including genetic information, whether oral or recorded in any form or medium, that relates to the past, present, or

future physical or mental health or condition of an individual and that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

(6) SECRETARY.—The term ''Secretary'' means the Secretary of Health and Human Services.

SEC. 4. PROMULGATION OF REGULATIONS FOR OPERATORS OF CONSUMER DEVICES, SERVICES, APPLICATIONS, AND SOFTWARE.

(a) IN GENERAL.—Not later than 6 months after the date on which the report is submitted under section 5(d), the Secretary, in consultation with the Chairman of the Federal Trade Commission, the National Coordinator, relevant stakeholders, and heads of such other Federal agencies as the Secretary considers appropriate, shall promulgate regulations to help strengthen privacy and security protections for consumers' personal health data that is collected, processed, analyzed, or used by consumer devices, services, applications, and software.

(b) REQUIREMENTS.—

(1) IN GENERAL.—The Secretary shall ensure that the regulations pursuant to subsection (a)—

(A) account for differences in the nature and sensitivity of the data collected or stored on

the consumer device, service, application, or software; and

(B) include such definitions for relevant terms that are necessary to accomplish the goals of the regulations set forth in subsection (a).

(2) REQUIREMENTS OF SECRETARY.—In the promulgation of regulations under subsection (a), the Secretary, to the extent practicable, shall—

(A) consider the findings in the report issued by the Department of Health and Human Services to Congress entitled ''Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA'', including findings regarding individuals' access rights, re-use of data by third parties, security standards applicable to data holders and users, confusion or ambiguity regarding terminology related to privacy and security protections, and the adequacy of collection, use, and disclosure limitations;

(B) consider other regulations and guidance issued by the Federal Trade Commission, and other regulations promulgated under section 264(c) of the Health Insurance Portability

and Accountability Act of 1996 (42 U.S.C. 1320d–2 note), subtitle D of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17921 et seq.), Genetic Information Nondiscrimination Act (Public Law 110–233, 122 Stat. 881), the Common Rule as contained in part 46 of title 45, Code of Federal Regulations, and other related Acts;

(C) consistent with paragraph (3), consider appropriate uniform standards for consent related to the handling of genetic data, biometric data, and personal health data;

(D) consider exceptions to consent requirements under subparagraph (C) for purposes that may include law enforcement, academic research or research for the sole purpose of assessing health care utilization and outcomes, emergency medical treatment, or determining paternity;

(E) consider appropriate minimum standards of security that may differ according to the nature and sensitivity of the data collected or stored on, or processed or transferred by, the consumer device, service, application, or software;

(F) consider appropriate standards for the de-identification of personal health data;

(G) consider appropriate limitations on the collection, use, or disclosure of personal health data to that which is directly relevant and necessary to accomplish a specified purpose;

(H) consult with the National Coordinator, the Commissioner of Food and Drugs, and the Chairman of the Federal Trade Commission; and

(I) provide for initial and ongoing outreach regarding regulations affecting industries, businesses, and individuals to ensure awareness of consumer privacy and security protections in the field of digital health technology.

(3) UNIFORM STANDARDS.—In the review of each of the areas described in paragraph (2)(C), the Secretary shall consider—

(A) the development of standards for obtaining user consent based on how information will be shared to ensure that prior to the collection, analysis, use, or disclosure of consumers' personal health data, an operator of a consumer device, service, application, or software specifies

the uses of the personal health data and who will have access to the information;

(B) the manner in which consent is obtained in a way that uses clear, concise, and well-organized language that is easily accessible, of reasonable length, at an appropriate level of readability, and clearly distinguishable from other matters;

(C) a process to limit the transfer of personal health data to third parties and provide consumers with greater control over how their personal health data is used for marketing purposes;

(D) secondary uses outside of the primary purpose of the service as initially indicated when consent was first obtained;

(E) a process to permit a withdrawal of consent to ensure that a user is able to remove consent for the terms of service for use of the consumer device, service, application, or software, including the collection and use of personal health data as easily as the user is able to give such consent;

(F) providing a right to access a copy of the personal health data that the operator has

collected, analyzed, or used, free of charge and in an electronic and easily accessible format, including a list of each entity that received the personal health data from the operator, whether through sale or other means; and

(G) providing a right to delete and amend personal health data, to the extent practicable, that the operator has collected, analyzed, or used.

(c) UPDATES.—The Secretary shall review and, if necessary, update the regulations promulgated under subsection (a) in accordance with the requirements under subsection (b).

(d) PUBLIC AVAILABILITY.—The Department of Health and Human Services shall make prominently available to the public on the Department's internet website, clear and concise information about available resources related to the regulations promulgated under subsection (a) and all updates to such resources.

(e) CONSISTENCY OF RESOURCES PUBLISHED BY FEDERAL AGENCIES.—If a Federal agency publishes resources to help protect consumers' personal health data, the head of such Federal agency, to the degree practicable, shall make such resources consistent with the regulations promulgated under subsection (a).

(f) OTHER FEDERAL PRIVACY AND SECURITY REQUIREMENTS.—Nothing in this section shall be construed to supersede, alter, or otherwise affect any privacy and security requirements enforced by Federal agencies.

SEC. 5. NATIONAL TASK FORCE ON HEALTH DATA PROTECTION.

(a) ESTABLISHMENT.—The Secretary, in consultation with the Chairman of the Federal Trade Commission, the National Coordinator, and relevant stakeholders, shall establish a task force, to be known as the National Task Force on Health Data Protection (referred to in this section as the ''Task Force'').

(b) DUTIES.—The Task Force shall—

(1) study the long-term effectiveness of de-identification methodologies for genetic data and biometric data;

(2) evaluate and provide input on the development of security standards, including encryption standards and transfer protocols, for consumer devices, services, applications, and software;

(3) evaluate and provide input with respect to addressing cybersecurity risks and security concerns related to consumer devices, services, applications, and software;

(4) evaluate and provide input with respect to the privacy concerns and protection standards related to consumer and employee health data;

(5) review and advise on the need, if any, to update the report issued by the Department of Health and Human Services to Congress entitled ''Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA''; and

(6) provide advice and consultation in the establishment and dissemination of resources to educate and advise consumers about the basics of genetics and direct-to-consumer genetic testing, and the risks, benefits, and limitations of such testing.

(c) MEMBERS.—The Secretary, in consultation with the Chairman of the Federal Trade Commission, the National Coordinator, and relevant stakeholders, shall appoint not more than 15 members to the Task Force. In appointing such members, the Secretary shall ensure that the total membership of the Task Force is an odd number and represents a diverse set of stakeholder perspectives.

(d) REPORTING.—Not later than 1 year after the date of enactment of this Act, the Task Force shall prepare and submit to the Committee on Commerce, Science, and Transportation of the Senate, the Committee on

Health, Education, Labor, and Pensions of the Senate, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Energy and Commerce of the House of Representatives, the Committee on Homeland Security of the House of Representatives, the Secretary, the Chairman of the Federal Trade Commission, and the Commissioner of Food and Drugs, a report on the findings of the Task Force.

(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as may be necessary to carry out this section.

(f) FEDERAL ADVISORY COMMITTEE ACT.—The Federal Advisory Committee Act (5 U.S.C. App.) shall apply to the Task Force.

(g) SUNSET.—

(1) IN GENERAL.—The Task Force shall terminate on the date that is 5 years after the date of the first meeting of the Task Force.

(2) RECOMMENDATION.—Not later than the date that is one year prior to the termination of the Task Force under paragraph (1), the Secretary shall submit to Congress a recommendation on whether the Task Force should be extended.

○