AMENDMENT NO. ____________________

Calendar No. ____________________

Purpose: To provide for the privacy and security of protected health information.


S. 1693

To enhance the adoption of a nationwide interoperable health information technology system and to improve the quality and reduce the costs of health care in the United States.

Referred to the Committee on ____________________ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT intended to be proposed by ____________________

Viz:

1. On page 85, between lines 9 and 10, insert the following:

   “(9) PROTECTED HEALTH INFORMATION.—The term ‘protected health information’ means any information, including genetic information, biometric information, demographic information, and tissue samples collected from an individual, whether oral or recorded in any form or medium, that—
“(A) is created or received by a health care provider, health researcher, health plan, health or life insurer, medical or health savings plan administrator, school or university, health care clearinghouse, health oversight agency, public health authority, employer, data broker, or other person or such person’s agent, officer, or employee;

“(B) relates to the past, present, or future physical or mental health or condition of an individual (including individual cells and their components), the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and

“(C)(i) identifies an individual; or

“(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify an individual.”.

On page 85, line 10, strike “(9)” and insert “(10)”.

On page 86, line 13, strike “(10)” and insert “(11)”.
On page 158, between line 17 and 18, insert the following:

SEC. 401. RIGHT OF SUBJECTS OF PROTECTED HEALTH INFORMATION.

Title XXX of the Public Health Service Act, as amended by section 301, is further amended by adding at the end the following:

“SEC. 3014. RIGHT TO PRIVACY AND SECURITY.

“(a) IN GENERAL.—In addition to the rights described in section 3013, individuals who are the subject of protected health information shall have the right to—

“(1) privacy and security with respect to the use and disclosure of such information;

“(2) control and withhold protected health information of which they are the subject; and

“(3) exercise nondisclosure and nonuse rights (referred to in this title as the right to ‘opt-out’) with respect to their protected health information, including the right to opt out of any local, regional, or nationwide health information network or system that is used by the individual.

“(b) OBLIGATIONS.—A person that discloses, uses, or receives an individual’s protected health information shall expressly recognize the right to privacy and security of
such individual with respect to the use and disclosure of such information.

“SEC. 3015. INSPECTION AND COPYING OF PROTECTED HEALTH INFORMATION.

“(a) Right of the Individual.—

“(1) In General.—A person, including a health care provider, health researcher, health plan, health or life insurer, medical or health savings plan administrator, school or university, health care clearinghouse, health oversight agency, public health authority, employer, or data broker, or such person’s agent, officer, employee, or affiliate, that accesses, maintains, retains, modifies, records, stores, or otherwise holds, uses, or discloses protected health information, shall permit an individual who is the subject of such protected health information, or the individual’s designee, to inspect and copy the protected health information concerning the individual, including records created under this section and section 3020.

“(2) Procedures and Fees.—A person described in paragraph (1) may establish appropriate procedures to be followed for the inspection and copying of information under such paragraph and may require an individual to pay reasonable fees as-
associated with such inspection and copying in an amount that does not exceed the actual costs of providing such copying. Such fees may not be assessed where such an assessment would have the effect of inhibiting an individual from gaining access to the information described in paragraph (1).

“(b) DEADLINE.—A person described in subsection (a)(1) shall comply with a request for inspection or copying of protected health information under this section by not later than—

“(1) 15 business days after the date on which the person receives the request, if such request requires the inspection, copying, or sending of printed materials; or

“(2) 5 business days after the date on which the person receives the request, or earlier if the Secretary determines appropriate, if such request requires only the inspection, copying, or sending of electronic or other digital materials.

“(c) RULES GOVERNING AGENTS.—A person that is the agent, officer, or employee of a person described in subsection (a) shall provide for the inspection and copying of protected health information if—

“(1) the protected health information is retained by the person; and
“(2) the person has been asked by the person described in subsection (a)(1) to fulfill the requirements of this section.

“(d) SPECIAL RULE RELATING TO ONGOING CLINICAL TRIALS.—With respect to protected health information that is created as part of an individual’s participation in an ongoing clinical trial, access to the information shall be provided consistent with the individual’s agreement to participate in the clinical trial.

“SEC. 3016. MODIFICATIONS TO PROTECTED HEALTH INFORMATION.

“(a) IN GENERAL.—Not later than 15 business days, or earlier if the Secretary determines appropriate, after the date on which a person described in section 3015(a)(1) receives from an individual a request in writing to supplement, correct, amend, segregate, or remove protected health information concerning the individual, such person shall—

“(1) subject to subsections (b) and (c), modify the information, by adding the requested supplement, correction, or amendment to the information, or by removing any information that has been requested to be destroyed;

“(2) inform the individual that the modification has been made; and
“(3) make reasonable efforts to inform any person to which the portion of the unmodified information was previously disclosed, of any substantive modification that has been made.

“(b) REFUSAL TO MODIFY.—If a person described in subsection (a) declines to make the modification requested under such subsection within 15 business days after receipt of such request, such person shall inform the individual involved in writing of—

“(1) the reasons for declining to make the modification;

“(2) any procedures for further review of the declining of such modification; and

“(3) the individual’s right to file with the person a concise statement setting forth the requested modification and the individual’s reasons for disagreeing with the declining person and the individual’s right to include a copy of such refusal in the health record set concerning the individual.

“(c) STATEMENT OF DISAGREEMENT.—If an individual has filed with a person a statement of disagreement under subsection (b)(3), the person, in any subsequent disclosure of the disputed portion of the information—
“(1) shall include, at the individual’s request, a copy of the individual’s statement in the individual’s health record set; and

“(2) may include a concise statement of the reasons for not making the requested modification.

“(d) RULES GOVERNING AGENTS.—A person that is the agent of a person described in subsection (a) shall only be required to make a modification to protected health information where—

“(1) the protected health information is retained, distributed, used, or maintained by the agent; and

“(2) the agent has been asked by such person to fulfill the requirements of this section.

“(e) NOTIFICATION OF LOSS OR CORRUPTION.—Not later than 15 business days, or earlier if the Secretary determines appropriate, after the date on which a person described in subsection (a) discovers the loss or corruption of health record sets or protected health information under its management, or if such person has reason to believe that its database has been compromised, such person shall—

“(1) notify individuals whose records have been affected;
“(2) notify persons and the agents of persons that receive, access, maintain, retain, modify, record, store, destroy, or otherwise use or disclose such data; and

“(3) repair or restore corrupted data to the extent practicable.

“SEC. 3017. NOTICE OF PRIVACY PRACTICES.

“(a) PREPARATION OF WRITTEN NOTICE.—A person described in section 3015(a)(1) shall prepare a written notice of the privacy practices of such person, including information with respect to the following:

“(1) The express right of an individual to privacy, security, and confidentiality with respect to the electronic disclosure of such individual’s protected health information.

“(2) The procedures for an individual to authorize disclosures of protected health information, and to object to, modify, and revoke such authorizations.

“(3) The right of an individual to inspect, copy, and modify that individual’s protected health information.

“(4) The right of an individual not to have employment or the receipt of services or choice of
health plan conditioned upon the execution by the individual of an authorization for disclosure.

“(5) A description of the categories or types of employees, by general category or by general job description, who have access to or use of protected health information regarding the individual.

“(6) A simple, concise description of any information systems used to store or transmit protected health information, including a description of any linkages made with other networks, systems, or databases outside the person’s direct control.

“(7) The right of and procedures for an individual to request segregation of protected health information, and to restrict the use of such information by employees, agents, and contractors of a person.

“(8) The circumstances under which the information will be, lawfully and actually, used or disclosed without an authorization executed by the individual.

“(9) A statement that, if an individual elects to pay for health care from the individual’s own funds, that individual may elect for identifying information not to be disclosed to anyone other than designated health care providers, unless such disclosure is re-
quired by mandatory reporting requirements or other similar information collection duties required by law.

“(10) The right of the individual to have continued maintenance, distribution, or storage of that individual’s personal health information not conditioned upon whether that individual amends or revokes an authorization for disclosure, or requests a modification of protected health information.

“(11) The right of and procedures for an individual to request that protected health information be transferred to a third party person without unreasonable delay.

“(12) The right to prompt notification of an actual or suspected security breach of protected health information, and how such breaches will be remedied by the person.

“(13) The right of an individual to inspect and obtain a copy of records of authorized and unauthorized disclosures as well as attempted and actual access and use by an authorized or unauthorized person.

“(14) The right of an individual to exercise nondisclosure and nonuse rights (referred to in this title as the right to ‘opt-out’) with respect to their
protected health information, including the right to
opt out of any local, regional, or nationwide health
information network or system that is used by the
person.

“(b) Provision and Posting of Written Notice.—

“(1) Provision.—A person described in sub-
section (a) shall provide a copy of the written notice
of privacy practices required under such sub-
section—

“(A) at the time an authorization is sought
for the disclosure of protected health informa-
tion; and

“(B) upon the request of an individual.

“(2) Posting.—A person described in sub-
section (a) shall post, in a clear and conspicuous
manner, a brief summary of the privacy practices of
the person.

“(c) Model Notice.—The Secretary, after notice
and opportunity for public comment, shall develop and dis-
seminate model notices of privacy practices, and model
summary notices for posting for use under this section.
Use of such model notice shall be deemed to satisfy the
requirements of this section.
“(d) REQUIREMENT FOR OPT-OUT.—A person shall not access, maintain, retain, modify, record, store, destroy, or otherwise use or disclose an individual’s protected health information for other than treatment or payment purposes until that individual has been given an opportunity, before the time that such information is initially used or disclosed, to direct that such information not be used or disclosed. The individual must be given adequate time to exercise the nondisclosure and nonuse option (the right to opt-out) through the method that is most convenient to the individual, along with an explanation of how the individual can exercise such option.

“SEC. 3018. DEMONSTRATION GRANT.

“(a) IN GENERAL.—The Secretary shall award contracts or competitive grants to eligible entities to support demonstration projects that are designed to improve the communication of information pertaining to health privacy rights with individuals with limited English language proficiency and limited health literacy.

“(b) PURPOSE.—It is the purpose of this section, to promote the cultural competency of persons that access, maintain, retain, modify, record, store, destroy, or otherwise use or disclose protected health information, and to enable such persons to better communicate privacy proce-
dures to non-English speakers, those with limited English proficiency, and those with limited health literacy.

“(c) ELIGIBLE ENTITIES.—In this section, the term ‘eligible entity’ means an organization or community-based consortium that includes—

“(1) individuals who are representatives of organizations serving or advocating for ethnic and racial minorities, low income immigrant populations, and others with limited English language proficiency and limited health literacy;

“(2) health care providers that provide care for ethnic and racial minorities, low income immigrant populations, and others with limited English language proficiency and limited health literacy;

“(3) community leaders and leaders of community-based organizations; and

“(4) experts and researchers in the areas of social and behavioral sciences, who have knowledge, training, or practical experience in health policy, advocacy, cultural and linguistic competency, or other relevant areas as determined by the Secretary.

“(d) APPLICATION.—An eligible entity seeking a contract or grant under this section shall submit an application to the Secretary at such time, in such manner, and containing such information as the Secretary may require.
“(e) Use of Funds.—An eligible entity shall use amounts received under this section to carry out programs and studies designed to help identify best practices in the communication of privacy rights and procedures to ensure comprehension by individuals with limited English proficiency and limited health literacy.

“Sec. 3019. Establishment of Safeguards.

“(a) In General.—A person described in section 3015(a)(1) shall establish and maintain appropriate administrative, organizational, technical, and physical safeguards and procedures to ensure the privacy, confidentiality, security, accuracy, and integrity of protected health information that is accessed, maintained, retained, modified, recorded, stored, destroyed, or otherwise used or disclosed by such person.

“(b) Factors to Be Considered.—The safeguards and procedures established under subsection (a) shall ensure that—

“(1) protected health information is used or disclosed only with informed consent;

“(2) the categories of personnel who will have access to protected health information are identified;

“(3) the feasibility of limiting access to protected health information is considered;
“(4) the privacy, security and confidentiality of protected health information is maintained;

“(5) protected health information is protected against any anticipated vulnerabilities to the privacy, security, or integrity of such information; and

“(6) protected health information is protected against unauthorized access, use, or misuse of such information.

“(c) MODEL GUIDELINES.—The Secretary, after notice and opportunity for public comment, shall develop and disseminate model guidelines for the establishment of safeguards and procedures for use under this section, such as, where appropriate, individual authentication of uses of computer systems, access controls, audit trails, encryption, physical security, protection of remote access points and protection of external electronic communications, periodic security assessments, incident reports, and sanctions. The Secretary, or his or her designee, shall update and disseminate the guidelines, as appropriate, to take advantage of new technologies.

“(d) REVIEW AND UPDATING OF SAFEGUARDS.—Persons subject to this title shall monitor, evaluate, and adjust, as appropriate, all safeguards and procedures, concomitant with relevant changes in technology, the sensitivity of personally identifiable information, internal or ex-
ternal threats to personally identifiable information, and any changes in the contracts or business of the person. For the purpose of reviewing and updating safeguards, the Secretary may provide technical assistance to persons described in subsection (a), as appropriate.

"SEC. 3020. TRANSPARENCY.

"(a) Public List of Data Brokers.—A person described in section 3015(a)(1) shall establish a list of data brokers with which such person has entered into a contract or relationship for the purposes of providing services involving any protected health information. Such list and the contact information for each broker shall be made publicly accessible on the Internet.

"(b) Subcontracting and Outsourcing Overseas.—In the event a person subject to this title contracts with service providers not subject to this title, including service providers operating in a foreign country, such person shall—

"(1) take reasonable steps to select and retain third party service providers capable of maintaining appropriate safeguards for the security, privacy, and integrity of protected health information;

"(2) require by contract that such service providers implement and maintain appropriate meas-
ures designed to meet the requirements of persons subject to this title;

“(3) be held liable for any violation of this title by an overseas service provider or other provider not subject to this title; and

“(4) in the case of a service provider operating in a foreign country, obtain the informed consent of the individual involved prior to outsourcing such individual’s protected health information to such provider.

“(c) List of Persons.—The Secretary shall maintain a public list identifying persons described in section 102(a)(1) that have lost, stolen, disclosed, or used in an unauthorized manner or for an unauthorized purpose the protected health information of a significant number of individuals. The list shall include how many individuals were affected by such action.

“SEC. 3021. RISK MANAGEMENT.

“(a) In General.—Persons described in section 3015(a)(1) that have access to protected health information shall establish risk management and control processes to protect against anticipated vulnerabilities to the privacy, security, and integrity of protected health information.
“(b) Risk Assessment.—A person described in subsection (a) shall perform annual risk assessments of procedures, systems, or networks involved in the creation, accessing, maintenance, retention, modification, recording, storage, distribution, destruction, or other use or disclosure of personal health information. Such risk assessment may include—

“(1) identifying reasonably foreseeable internal and external vulnerabilities that could result in inaccuracy or in unauthorized access, disclosure, use, or modification of protected health information, or of systems containing protected health information;

“(2) assessing the likelihood of and potential damage from inaccuracy or from unauthorized access, disclosure, use, or modification of protected health information;

“(3) assessing the sufficiency of policies, technologies, and safeguards in place to minimize and control risks from unauthorized access, disclosure, use, or modification of protected health information; and

“(4) assessing the vulnerability of protected health information during destruction and disposal of such information, including through the disposal or retirement of hardware.
“(c) Risk Management.—A person described in subsection (a) shall establish risk management and control procedures designed to control risks such as those identified in subsection (b). Such procedures shall include—

“(1) a means for the detection and recording of actual or attempted, unauthorized, fraudulent, or otherwise unlawful access, disclosure, transmission, modification, use, or loss of personal health information;

“(2) procedures for ensuring the secure disposal of personal health information;

“(3) a means for limiting physical access to hardware, software, data storage technology, servers, systems, or networks by unauthorized persons in order to minimize the risk of information disclosure, modification, transmission, access, use, or loss;

“(4) providing appropriate risk management and control training for employees; and

“(5) carrying out annual testing of such risk management and control procedures.

“Sec. 3022. Accounting for Disclosures and Use.

“(a) In General.—A person described in section 3015(a)(1) shall establish and maintain, with respect to any protected health information disclosure, a record of each disclosure in accordance with regulations promul-
gated by the Secretary. Such record shall include the purpose of any disclosure and the identity of the specific individual executing the disclosure, as well as the person to which such information is disclosed.

“(b) MAINTENANCE OF RECORD.—A record established under subsection (a) shall be maintained for not less than 7 years.

“(c) ELECTRONIC RECORDS.—A person described in subsection (a) shall, to the maximum extent practicable, maintain an accessible electronic record concerning each access, use, or disclosure, whether authorized or unauthorized and whether successful or unsuccessful, of protected health information maintained by such person in electronic form. The record shall include the identities of the specific individuals (or a way to identify such individuals, or information helpful in determining the identities of such individuals) who access or seek to gain access to, use or seek to use, or disclose or seek to disclose, information sufficient to identify the protected health information sought or accessed, and other appropriate information.

“(d) ACCESS TO RECORDS.—A person described in subsection (a) shall permit an individual who is the subject of protected health information, or the individual’s designee, to inspect and copy the records created under subsection (a) and (c).”.