.....

(Original Signature of Member)

110TH CONGRESS
2ND SESSION

H. R. _____

To provide individuals with access to health information of which they are a subject, to ensure personal privacy, security, and confidentiality with respect to health related information in promoting the development of a nationwide interoperable health information infrastructure, to impose criminal and civil penalties for unauthorized use of personal health information, to provide for the strong enforcement of these rights, to protect States' rights, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. MARKEY introduced the following bill; which was referred to the Committee on _____

A BILL

To provide individuals with access to health information of which they are a subject, to ensure personal privacy, security, and confidentiality with respect to health related information in promoting the development of a nationwide interoperable health information infrastructure, to impose criminal and civil penalties for unauthorized use of personal health information, to provide for the strong enforcement of these rights, to protect States' rights, 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. SHORT TITLE.

(a) SHORT TITLE.—This Act may be cited as the ''Technologies for Restoring Users' Security and Trust in Health Information Act of 2008'' or as the ''TRUST in Health Information Act of 2008''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

SEC. 2. FINDINGS; PURPOSES.

(a) FINDINGS.—Congress finds the following:

(1) Americans are deeply concerned about the privacy and security of their personal information, including their health records.

(2) In October 2007, a Harris Interactive Poll commissioned by the Institute of Medicine found that 58 percent of respondents indicated they do not believe Federal and State laws and organizational practices offer sufficient protection of personal health information.

(3) In February 2007, the Markle Foundation reported that 80 percent of individuals surveyed were very concerned about identity theft or fraud and 77 percent were very concerned that their medical information would be used for marketing purposes.

(4) Concerns about the privacy and security of personal health information are fueled by the escalating number of breaches of personal information that have occurred in recent years and numerous reports of the inadequacy of the security of electronic networks.

(5) According to the Privacy Rights Clearinghouse, more than 216,000,000 data records belonging to U.S. residents have been exposed to potential misuse as a result of security breaches since January 2005.

(6) A nationwide interoperable health information infrastructure can strengthen privacy, security, and confidentiality safeguards, protecting patients' personal health information while also improving health care quality, safety, and affordability.

(7) In order for individuals, health care providers, and health care payers to achieve the benefits associated with such infrastructure, strong data privacy, security, and confidentiality standards must be developed, adopted, and incorporated into the health information technology infrastructure.

(8) While Executive Order 13335 regarding interoperable health information technology issued on April 27, 2004, called for widespread adoption of interoperable electronic health records within 10 years, established the position of National Coordinator of Health Information Technology, and stipulated that the plan for the nationwide implementation of interoperable health information technology should address privacy and security issues, adequate

progress has not been made to ensure that a strong data privacy, security, and confidentiality approach will guide the development of this nationwide infrastructure beginning in its initial stages and continuing throughout its formulation.

(9) According to a February 1, 2007, report of the Government Accountability Office (GAO), the Department of Health and Human Services and its Office of the National Coordinator of Health Information Technology have not yet defined an overall approach for integrating privacy-related initiatives the Department has undertaken in the area of health information technology or addressing key privacy principles, nor has the Department defined milestones for integrating the results of these activities while it has moved forward with development of standards for a national electronic health information system.

(10) All Americans have a right to privacy, security, and confidentiality with respect to the electronic disclosure of their personal health information, and the nationwide implementation of interoperable health information technology should abide by, and be consistent with, this right.

(11) Without adequate privacy, security, and confidentiality standards, individuals will be more likely to avoid or delay medical treatment or withhold pertinent information from their health providers, potentially resulting in lost productivity, increased morbidity rates, and increased costs to the health care system.

(12) As stipulated by the Secretary of Health and Human Services in the Final Rule for Standards for Privacy of Individually Identifiable Health Information (45 C.F.R. parts 160 and 164), the standards contained in the Final Rule are intended to establish a floor of privacy protection and are not designed to serve as ''best practices'' for the use or disclosure of personal health information.

(13) To guide the development, implementation, and operation of an interoperable nationwide health information technology infrastructure, Congress should establish specific minimum standards for the use and disclosure of individuals' personal health information and direct the Department of Health and Human Services to promulgate regulations relating to personal health information that are consistent with individuals' right to privacy, security, and confidentiality with respect to the electronic use or dis-

closure of their personal health information, the public interest, and the purposes of this Act.

(b) PURPOSE.—The purposes of this Act are as follows:

(1) To recognize that individuals have a right to privacy, confidentiality, and security with respect to health information, including genetic information, and that those fundamental rights are rooted in the Nation's history and medical ethics and must be protected.

(2) To ensure that individuals are able to exercise their right to health information privacy by requiring their consent for the use and disclosure of their identifiable health information unless otherwise required by law

(3) To encourage the development of a nationwide interoperable health information technology infrastructure that protects individuals' privacy, confidentiality, and security with respect to their health information while also improving health care quality, promoting data accuracy, reducing medical errors, and increasing the efficiency of care.

(4) To create incentives to turn personal health information into de-identified health information (as defined in section 171(5)), where appropriate.

(5) To designate an Office of Health Information Privacy within the Department of Health and Human Services to protect individuals' right of privacy.

(6) To provide individuals with—

(A) access to health information of which they are the subject;

(B) the opportunity to challenge the accuracy and completeness of such information by being able to file modifications to or request the deletion of such information; and

(C) the right to limit the use and disclosure of personal health information.

(7) To establish strong and effective mechanisms to protect against the unauthorized and inappropriate use of personal health information and ensure that these mechanisms safeguard this information wherever it may reside.

(8) To provide notice to individuals of breaches of their personal health information.

(9) To invoke the sweep of congressional powers, including the power to enforce the 14th Amendment to the Constitution, to regulate commerce, and to abrogate the immunity of the States under the 11th Amendment to the Constitution, in order to ad-

dress violations of the rights of individuals to privacy, to provide individuals with access to their health information, and to prevent the unauthorized use of personal health information that is genetic information.

(10) To establish strong and effective remedies for violations of this Act.

(11) To protect the rights of States.

TITLE I—HEALTH INFORMATION PRIVACY AND SECURITY

SEC. 100. SUMMARY OF PRIVACY RIGHTS AND SECURITY OBLIGATIONS.

(a) PRIVACY RIGHTS.—In order to provide individuals who are the subject of personal health information with privacy, security, and control in the use and disclosure of such information, such individuals are provided the following rights under this title:

(1) The right to not have their personal health information disclosed without their informed consent unless otherwise required by law, pursuant to subtitle C.

(2) The right to inspect and copy their personal health information, pursuant to section 101.

(3) The right to correct, supplement, or remove their personal information held by a person, pursuant to section 102.

(4) The right to prohibit access by certain categories of persons to particularly sensitive personal health information about individuals, such as information relating to mental health, domestic violence, sexually transmitted diseases, and infection with the human immunodeficiency virus (HIV), pursuant to section 122.

(5) The right to receive notification of actual or suspected security breaches of their personal health information, pursuant to section 113.

(6) The right to receive an accounting of all electronic disclosures of their personal health information upon request, pursuant to section 116.

(b) SECURITY OBLIGATIONS.—A person that discloses, uses, or receives an individual's personal health information has obligations under this title, including the following:

(1) The obligation to expressly recognize the right to privacy and security of such individual with respect to the use and disclosure of such information under subtitle B.

(2) The obligation to permit individuals who are the subject of such personal health information to inspect and copy the personal health information concerning the individual pursuant to section 101.

(3) The obligation to provide written notification to an individual of the person's privacy practices pursuant to section 111.

(4) The obligation to promptly notify individuals of an actual or suspected security breach of their personal health information pursuant to section 113.

(5) The obligation to establish and maintain appropriate administrative, organizational, technical and physical safeguards to ensure the privacy, confidentiality, security, accuracy, and integrity of personal health information that is accessed, maintained, modified, recorded, stored, destroyed, or otherwise used or disclosed by such person pursuant to section 112.

(6) The obligation to make publicly available on the Internet a list, including contact information, of each data partner with which the person has entered into a contract or relationship to provide services involving personal health information pursuant to section 114.

(7) The obligation to obtain an individual's informed consent or authorization before using or disclosing an individual's personal health information pursuant to chapter 1 of subtitle C.

(8) The obligation to establish and update risk management processes to protect against vulnerabilities to the privacy and security of individual's personal health information pursuant to sections 112 and 114.

(9) The obligation to establish and maintain a record of each disclosure of an individual's personal health information pursuant to section 116.

(10) The obligation to provide individuals with concise, comprehensive, and explicit information if seeking to use or disclose their personal health information for marketing purposes and receive a separate authorization from an individual before using or disclosing the information for that purpose pursuant to section 123.

Subtitle A—Access to and Accuracy of Personal Health Information

SEC. 101. INSPECTION AND COPYING OF PERSONAL HEALTH INFORMATION.

(a) RIGHT OF INDIVIDUAL.—

(1) IN GENERAL.—A health information person (as defined in section 171(13)) shall permit an individual who is the subject of personal health information (as defined in section 171(23)) that the person holds, uses, or discloses, or the individual's designee, to inspect and copy the personal health information concerning the individual.

(2) PROCEDURES AND FEES.—A health information person may establish appropriate procedures to be followed for inspection and copying under paragraph (1) and may require an individual to pay reasonable fees associated with such inspection and copying in an amount that is not in excess of 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 health information person shall comply with a request for inspection or copying of personal health information under this section 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 sooner 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 health information person shall provide for the inspection and copying of personal health information if—

(1) the personal health information is retained by the person; and

(2) the person has been asked by the health information person to fulfill the requirements of this section.

(d) SPECIAL RULE RELATING TO ONGOING CLINICAL TRIALS.—With respect to personal health information that is created as part of an individual's voluntary participation in an ongoing clinical trial, access to the information shall be provided within 15 business days after the date on which the health information person receives the request or consistent with the individual's agreement to participate in the clinical trial, whichever is sooner.

SEC. 102. MODIFICATIONS TO PERSONAL HEALTH INFORMATION.

(a) IN GENERAL.—Not later than 15 business days, or earlier if the Secretary determines appropriate, after the date on which a health information person receives from an individual a request in writing to supplement, correct, amend, segregate, or remove personal health information that the person holds, uses, or discloses concerning the individual, such person—

(1) shall, 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) shall inform the individual that the modification has been made; and

(3) shall 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 health information person declines to make the modification requested under subsection (a) within 15 business days after receipt of such request, such person shall inform the individual 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 this refusal in the health record set (as defined in section 171(17)) concerning the individual.

(c) STATEMENT OF DISAGREEMENT.—If an individual has filed with a health information 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 health information person shall only be required to make a modification to personal health information where—

(1) the personal 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.

Subtitle B—Security of Personal Health Information

SEC. 111. NOTICE OF PRIVACY PRACTICES.

(a) PREPARATION OF WRITTEN NOTICE.—A health information person 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 disclosure of such individual's personal health information.

(2) The procedures for an individual to exercise that right by authorizing disclosures of personal 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 personal 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, except as permitted by section 122(c).

(5) A description of—

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

(B) the right of the individual to limit access to or use of his or her personal health information by employees, agents, and contractors of the person; and

(C) the procedures for effecting such limitations.

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

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

(8) A statement that, if an individual elects to pay for health care from the individual's own funds, that individual may elect for personal health infor-

mation, including any identifying information, not to be disclosed to anyone other than designated health care providers, unless such disclosure is required by mandatory reporting requirements or other similar information collection duties required by law.

(9) 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 personal health information.

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

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

(12) 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.

(13) The right of an individual to exercise non-disclosure and nonuse rights with respect to their personal 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 health information person shall provide in writing a copy of the notice of privacy practices required under subsection (a)—

(A) at the first contact between the individual and the person; and

(B) upon the request of an individual.

(2) POSTING.—A health information person shall post, in a clear and conspicuous manner, a brief summary of the privacy practices of the person.

(c) MODEL NOTICE.—The Secretary, in consultation with the Director of the Office of Health Information Privacy, after notice and opportunity for public comment, shall develop and disseminate 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.

SEC. 112. ESTABLISHMENT OF SAFEGUARDS.

(a) IN GENERAL.—A health information person shall—

(1) establish and maintain appropriate administrative, organizational, technical, and physical safeguards and procedures to ensure the privacy, confidentiality, security, accuracy, and integrity of personal health information that is accessed, maintained, retained, modified, recorded, stored, destroyed, or otherwise held, used, or disclosed by such person; and

(2) employ an individual whose responsibilities include the management of the person's information security.

(b) FACTORS TO BE CONSIDERED.—The policies and safeguards established under subsection (a) shall ensure that—

(1) personal health information is used or disclosed only with informed consent (as defined in section 171(19));

(2) the categories of personnel who will, with the informed consent of the individual, have access to personal health information are identified;

(3) the feasibility of limiting access to personal health information is considered;

(4) the privacy, security, and confidentiality of personal health information is maintained;

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

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

(c) MODEL GUIDELINES.—The Secretary, in consultation with the Director of the Office of Health Information Privacy appointed under section 161, after notice and opportunity for public comment, in accordance with the requirements of chapter 5 of title 5, United States Code, 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 or any additional security methodology or technology other than encryption which renders data in electronic form unreadable or indecipherable, physical security, protection of remote access points and protection of external electronic communications, periodic security assessments, incident reports, and sanctions. The Secretary, in consultation with the Director, shall up-

date and disseminate the guidelines, as appropriate, to take advantage of new technologies, so as to ensure that the .guidelines emphasize the need for stringent privacy, security, and confidentiality safeguards and procedures.

(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 external 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 health information persons, as appropriate.

SEC. 113. NOTIFICATION IN THE CASE OF BREACH.

(a) IN GENERAL.—A health information person that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses personal health information shall, following the discovery of a security breach (as defined in section 171(28)) of such information, notify each individual whose personal health information has been, or is reasonably believed to have been, accessed, or acquired during such breach.

(b) OBLIGATION OF OWNER OR LICENSEE.—

(1) NOTICE TO OWNER OR LICENSEE.—Any person engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects personal health information that the person does not own or license shall notify the owner or licensee of the information following the discovery of a security breach involving such information.

(2) NOTICE BY OWNER, LICENSEE, OR OTHER DESIGNATED THIRD PARTY.—Nothing in this subtitle shall be construed to prevent or abrogate an agreement between a person required to give notice under this section and a designated third party, including an owner or licensee of the personal health information subject to the security breach, to provide the notifications required under subsection (a).

(3) PERSON RELIEVED FROM GIVING NOTICE.—A person obligated to give notice under subsection (a) shall be relieved of such obligation if an owner or licensee of the personal health information subject to the security breach, or other designated third party, provides such notification.

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—All notifications required under this section shall be made within 15 business days, or earlier if the Secretary determines appro-

priate, following the discovery by the person of a security breach.

(2) BURDEN OF PROOF.—The person required to provide notification under this section shall have the burden of demonstrating that all notifications were made as required under this subtitle, including evidence demonstrating the necessity of any delay.

(d) METHODS OF NOTICE.—A person described in subsection (a) shall provide to an individual the following forms of notice in the case of a security breach:

(1) INDIVIDUAL NOTICE.—Notice required under this section shall be provided in such form as the individual selects, including—

(A) written notification to the last known home mailing address of the individual in the records of the person;

(B) telephone notice to the individual personally; or

(C) e-mail notice, if the individual has consented to receive such notice and the notice is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).

(2) MEDIA NOTICE.—Notice shall be provided to prominent media outlets serving a State or jurisdiction, if the personal health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, acquired by an unauthorized person.

(3) NOTICE TO SECRETARY.—Notice shall be provided to the Secretary for health information persons that have lost, stolen, disclosed, or used in an unauthorized manner or for an unauthorized purpose the personal health information of a significant number of individuals.

(e) CONTENT OF NOTIFICATION.—Regardless of the method by which notice is provided to individuals under this section, notice of a security breach shall include, to the extent possible—

(1) a description of the personal health information that has been, or is reasonably believed to have been, accessed, disclosed, or otherwise used by an unauthorized person;

(2) a toll-free number that the individual may use to contact the person described in subsection (a) to learn what types of personal health information the person maintained about that individual; and

(3) toll-free contact telephone numbers and addresses for major credit reporting agencies.

(f) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT PURPOSES.—

(1) IN GENERAL.—If a Federal law enforcement agency determines that the notification required under this section would impede a criminal investigation or cause damage to national security, such notification shall be delayed upon written notice from the Federal law enforcement agency to the person that experienced the breach.

(2) EXTENDED DELAY OF NOTIFICATION.—If the notification required under subsection (a) is delayed pursuant to paragraph (1), a person shall give notice not later than 30 days after such law enforcement delay was invoked unless a Federal law enforcement agency provides written notification that further delay is necessary.

SEC. 114. TRANSPARENCY.

(a) PUBLIC LIST OF DATA PARTNERS.—

(1) IN GENERAL.—A health information person shall establish a list of data partners (as defined in paragraph (2))) with which such person has entered into a contract or relationship for the purposes of providing services involving any personal health in-

formation held, used, or disclosed by the person. Such list and the contact information for each partner shall be made publicly accessible on the Internet.

(2) DATA PARTNER DEFINED.—In paragraph (1), the term ''data partner'' means a data bank, data warehouse, information clearinghouse, record locator system, or other business entity, which for monetary fees, dues, or on a cooperative nonprofit basis, engages in the practice of accessing, collecting, maintaining, modifying, storing, recording, transmitting, destroying, or otherwise using or disclosing the personal health information of individuals. Any person maintaining personal health information for the purposes of making such information available to the individual or the health care provider, including persons furnishing free or paid personal health records, electronic health records, electronic medical records, and related products and services, shall be deemed to be a data partner subject to the requirements of this title.

(b) SUBCONTRACTING AND OUTSOURCING OVERSEAS.—In the event a health information person 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 personal health information;

(2) require by contract that such service providers implement and maintain appropriate measures designed to meet the requirements applicable to health information persons under 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 personal health information to such provider.

(c) LIST OF PERSONS.—The Secretary shall maintain a public list identifying health information persons that have lost, stolen, disclosed, or used in an unauthorized manner or for an unauthorized purpose the personal health information of 1,000 or more individuals. The list shall include how many individuals were affected by such action and be displayed on the Web site of the Department of Health and Human Services.

SEC. 115. RISK MANAGEMENT.

(a) IN GENERAL.—Each health information person shall establish risk management and control processes to protect against anticipated vulnerabilities to the privacy, security, and integrity of personal health information that the person accesses, holds, uses, or discloses.

(b) RISK ASSESSMENT.—A health information person 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 shall include—

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

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

(3) assessing the sufficiency of policies, technologies, and safeguards in place to enable compliance with individuals' informed consent to the access, disclosure, use, or modification of their per-

sonal health information and minimize and control risks from unauthorized access, disclosure, use, or modification of individuals' personal health information; and

(4) assessing the vulnerability of personal health information during destruction and disposal of such information, including through the disposal or retirement of hardware.

(c) RISK MANAGEMENT.—A health information person 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. 116. ACCOUNTING FOR DISCLOSURES AND USE.

(a) IN GENERAL.—A health information person shall establish and maintain, with respect to any personal health information disclosure, a record of each disclosure in accordance with regulations promulgated by the Secretary in consultation with the Director of the Office of Health Information Privacy. 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 6 years.

(c) ELECTRONIC RECORDS.—A health information person 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 personal 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 informa-

tion 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 personal health information sought or accessed, and other appropriate information.

(d) ACCESS TO RECORDS.—A health information person shall permit an individual who is the subject of personal health information, or the individual's designee, to inspect and copy the records created in subsections (a) and (c).

Subtitle C—Use and Disclosure of Personal Health Information

CHAPTER 1—GENERAL RESTRICTIONS

SEC. 121. GENERAL RULES REGARDING USE AND DISCLOSURE.

(a) PROHIBITION.—

(1) GENERAL RULE.—A person may not disclose, access, or use personal health information except as authorized under this title.

(2) RULE OF CONSTRUCTION.—Disclosure or use of health information that meets the standards of being de-identified health information shall not be construed as a disclosure or use of personal health information.

(b) SCOPE OF DISCLOSURE OR USE.—

(1) IN GENERAL.—A disclosure or use of personal health information under this subtitle shall be limited to the minimum amount of information necessary to accomplish the purpose for which the disclosure or use is made, such as the individual's name and address, date of service, place of service, type of service, cost of service, and diagnosis.

(2) DETERMINATION.—The determination as to what constitutes the minimum disclosure or use possible for purposes of paragraph (1) shall be made by the individual or entity holding the information. The minimum necessary standard is intended to be consistent with, and not override, professional judgment and standards.

(c) USE OR DISCLOSURE FOR PURPOSE ONLY.—

(1) IN GENERAL.—An authorized recipient (as defined in paragraph (2)) of information pursuant to this subtitle may use or disclose such information solely to carry out the purpose for which the information was disclosed, except as provided in section 143.

(2) AUTHORIZED RECIPIENT DEFINED.—In paragraph (1), the term ''authorized recipient'' means a person granted the authority by an individual, in accordance with this title, to access, main-

tain, retain, modify, record, store, destroy, or otherwise use the individual's personal health information through an authorized disclosure.

(d) NO GENERAL REQUIREMENT TO DISCLOSE.—Nothing in this subtitle permitting the disclosure of personal health information shall be construed to require such disclosure.

(e) IDENTIFICATION OF DISCLOSED INFORMATION AS PERSONAL HEALTH INFORMATION.—Personal health information disclosed or used pursuant to this subtitle shall be clearly identified and labeled as personal health information that is subject to this title.

(f) DISCLOSURE OR USE BY AGENTS.—An agent, employee, or affiliate of a health information person that accesses, seeks to access, obtains, discloses, uses, or receives personal health information from such person, shall be subject to this subtitle to the same extent as the person.

(g) DISCLOSURE OR USE BY OTHERS.—A person receiving personal health information initially held by a person described in subsection (f) shall be subject to this subtitle to the same extent as the person described in subsection (f).

(h) CREATION OF DE-IDENTIFIED INFORMATION.—Notwithstanding subsection (c), but subject to the other provisions of this section, a person described in subsection

(f) may disclose personal health information to an employee or other agent of the person for purposes of creating de-identified information.

(i) UNAUTHORIZED USE OR DISCLOSURE OF THE DECRYPTION KEY.—The unauthorized disclosure of a decryption key (as defined in section 171(7)) or other secondary or tertiary means for accessing personal health information shall be deemed for purposes of this subtitle to be a disclosure of personal health information. The unauthorized use of a decryption key (or other secondary or tertiary means for accessing personal health information) or de-identified health information in order to identify an individual is deemed for purposes of this subtitle to be disclosure of personal health information.

(j) NO WAIVER.—Except as provided in this title, an informed consent or other authorization to disclose or use personally identifiable health information executed by an individual pursuant to this subtitle shall not be construed as a waiver of any rights that the individual has under other Federal or State laws, the rules of evidence, or common law.

(k) OPT-IN TO NETWORK SHARING.—

(1) IN GENERAL.—Before a health information person may share personal health information, through disclosure, access, use, or otherwise, with a

health information network or system, the individual must opt in to the sharing of such information with such network or system.

(2) HEALTH INFORMATION NETWORK OR SYSTEM DEFINED.—In this subsection, the term ''health information network or system'' means an interoperable health information infrastructure consisting of health information systems and other networks that connect providers, consumers, and others involved in supporting health and health care.

(l) DISPOSAL OF DATA.—To prevent the unauthorized disclosure or use of personal health information, such information, when disposed of, shall be de-identified, destroyed, or expunged from any electronic, paper, or other files and documents maintained by authorized persons to make such information permanently unreadable and undecipherable.

(m) OBLIGATIONS OF UNAUTHORIZED RECIPIENTS.—A person that obtains, accesses, or receives personal health information and that is an unauthorized recipient of such information may not access, maintain, retain, modify, record, store, destroy, or otherwise use or disclose such information for any purposes, and use or disclosure of personal health information under such circumstances shall be deemed for purposes of this subtitle

an unauthorized disclosure of personal health information, unless the disclosure is for the purpose of informing the Secretary, law enforcement authorities, or Congress of the person's unauthorized receipt of the personal health information.

SEC. 122. INFORMED CONSENT FOR DISCLOSURE OF PERSONAL HEALTH INFORMATION FOR TREATMENT AND PAYMENT.

(a) REQUIREMENTS RELATING TO EMPLOYERS, HEALTH PLANS, HEALTH OR LIFE INSURERS, UNINSURED AND SELF-PAY INDIVIDUALS, AND PROVIDERS.—

(1) IN GENERAL.—An employer, health plan, health or life insurer, or health care provider that seeks to disclose personal health information in connection with treatment or payment shall obtain informed consent (as defined in section 171(19)) from the subject of such personal health information that satisfies the requirements of this section. A single consent may authorize multiple disclosures.

(2) HEALTH PLANS, HEALTH OR LIFE INSURERS.—Every health plan or health or life insurer offering enrollment to individual or nonemployer groups shall, at the time of enrollment in the plan or insurance, obtain an informed consent for the use and disclosure of personal health information with

respect to each individual who is eligible to receive care or benefits under the plan or insurance.

(3) UNINSURED AND SELF-PAY.—An originating provider that provides health care in other than a network plan setting, or provides health care to an uninsured individual, shall obtain an informed consent for access to or use of personal health information in providing health care or arranging for health care from other providers or seeking payment for the provision of health care services.

(4) PROVIDERS.—Every health care provider that provides health care to an individual that has not been given the appropriate prior consent under this section, shall at the time of providing such care, or at such time as is practicable if services are necessary prior to the opportunity to obtain consent, obtain an informed consent for the use and disclosure of personal health information with respect to such individual.

(b) REQUIREMENTS FOR INDIVIDUAL INFORMED CONSENT.—To satisfy the requirements of this subsection, an informed consent from an individual to disclose the individual's personal health information shall—

(1) identify, by general job description or other functional description and by geographic location,

those persons that are authorized to disclose the information, including entities employed by a person authorized to disclose the information;

(2) describe the specific nature of the information to be disclosed;

(3) identify, by general job description or other functional description and by geographic location, those persons to which the information will be disclosed, including entities employed by a person to which information is authorized to be disclosed;

(4) describe the purpose of the disclosures;

(5) permit the executing individual to indicate that a particular person or class of persons (a group of persons with similar roles or functions) listed on the informed consent is not authorized to receive personal health information concerning the individual, except as provided for in subsection (c)(3);

(6) provide the means by which an individual may indicate that some of the individual's personal health information should be segregated and to what persons or classes of persons such segregated information may be disclosed;

(7) be subject to revocation by the individual and indicate that the informed consent is valid until

revocation by the individual or until an event or date specified;

(8)(A) be in writing, dated, and signed by the individual; and

(B) not have been revoked under subsection (f);

(9) describe the procedure by which an individual can amend an informed consent previously obtained by a person;

(10) describe the extent to which the authorized person will share information with sub-contracted persons, and the geographic location of sub-contracted persons, including those operating or located overseas, except that the authorized person shall obtain the informed consent of the individual involved prior to outsourcing such individual's personal health information to a sub-contracted person operating or located overseas; and

(11) describe the nature and probability of harm to the individual resulting from the informed consent for use or disclosure, consistent with the principle of informed consent.

(c) LIMITATION ON INFORMED CONSENT.—

(1) IN GENERAL.—Subject to paragraphs (2) and (3), a health information person that seeks informed consent under this subtitle may not condition

the delivery of treatment or payment for services on the receipt of such an informed consent.

(2) RIGHT TO REQUIRE SELF-PAYMENT.—

(A) IN GENERAL.—If an individual has refused to provide an informed consent for disclosure of administrative billing information (as defined in subparagraph (B)) to a person and such informed consent is necessary for a health care provider to receive payment for services delivered, the health care provider may require the individual to pay from their own funds for the services.

(B) ADMINISTRATIVE BILLING INFORMATION.—In subparagraph (A), the term ''administrative billing information'' means any of the following forms of personal health information:

(i) Date of service, policy, patient identifiers, and practitioner or facility identifiers.

(ii) Diagnostic codes, in accordance with medicare billing codes, for which treatment is being rendered or requested.

(iii) Complexity of service codes, indicating duration of treatment.

(iv) Total billed charges.

(3) RIGHT OF HEALTH CARE PROVIDER TO REQUIRE INFORMED CONSENT FOR TREATMENT PURPOSES.—If a health care provider that is seeking an informed consent for disclosure of an individual's personal health information believes that the disclosure of such information is necessary so as not to endanger the health or treatment of the individual, and if the withholding of services will not endanger the life of the individual, the health care provider may condition the provision of services upon the individual's execution of an informed consent to disclose personal health information to the minimum extent necessary.

(4) INFORMED CONSENTS FOR PAYMENT UNDER CERTAIN CIRCUMSTANCES.—If an individual is in a physical or mental condition such that the individual is not capable of authorizing the disclosure of personal health information and no other arrangements have been made to pay for the health care services being rendered to the patient, such information may be disclosed to a governmental authority to the extent necessary to determine the individual's eligibility for, and to obtain, payment under a governmental program for health care services provided to the patient. The information may also be dis-

closed to another provider of health care or health care service plan as necessary to assist the other provider or health care service plan in obtaining payment for health care services rendered by that provider of health care or health care service plan to the patient.

(d) MODEL INFORMED CONSENT.—The Secretary, in consultation with the Director of the Office of Health Information Privacy, after notice and opportunity for public comment in accordance with section 553 of title 5, United States Code, shall develop and disseminate model written informed consents of the type described in this section, which represent informed consent from the subject of such personal health information that satisfies the requirements of this section, and model statements of the limitations on informed consents. Any informed consent obtained on a model informed consent form under this section developed by the Secretary pursuant to the preceding sentence shall be deemed to satisfy the requirements for an informed consent under this section.

(e) SEGREGATION OF FILES.—A health information person shall comply with the request of an individual who is the subject of personal health information—

(1) to hide, mask, or mark separate any type or amount of personal health information held by the person; and

(2) to limit the use or disclosure of the segregated health information within the person to those specifically designated by the subject of the personal health information.

(f) REVOCATION OF INFORMED CONSENT.—

(1) IN GENERAL.—An individual may revoke or amend in writing an informed consent under this section at any time, unless the disclosure that is the subject of the consent is required to effectuate payment for health care that has been provided to the individual and for which the individual has declined or refused to pay from the individual's own funds.

(2) HEALTH PLAN.—With respect to a health plan, the informed consent of an individual is deemed to be revoked at the time of the cancellation or non-renewal of enrollment in the health plan, except as may be necessary to complete plan administration and payment requirements related to the individual's period of enrollment.

(g) RECORD OF INDIVIDUAL'S INFORMED CONSENTS AND REVOCATIONS.—Each person accessing, maintaining, retaining, modifying, recording, storing, destroying, or

otherwise using personally identifiable or personal health information for purposes of treatment or payment shall maintain a record for a period of 6 years of each informed consent by an individual and any revocation thereof, and such record shall become part of the individual's health record set.

SEC. 123. INFORMED CONSENT AND AUTHORIZATION FOR DISCLOSURE OF PERSONAL HEALTH INFORMATION OTHER THAN FOR TREATMENT OR PAYMENT.

(a) IN GENERAL.—A health information person that seeks to disclose personal health information for a purpose other than treatment or payment shall obtain informed consent. Such consent under this section shall be separate from an informed consent provided under section 122.

(b) LIMITATION ON AUTHORIZATIONS.—A person subject to section 122 may not condition the delivery of treatment, or payment for services, on the receipt of an informed consent or authorization described in this section.

(c) MODEL INFORMED CONSENTS AND AUTHORIZATIONS.—The Secretary, in consultation with the Director of the Office of Health Information Privacy, after notice and opportunity for public comment in accordance with section 553 of title 5, United States Code, shall develop

and disseminate model informed consents of the type described in subsection (a) and written authorizations of the type described in subsections (d) and (e). Any consent or authorization obtained on a respective model form shall be deemed to meet the requirements under the respective subsection.

(d) REQUIREMENT OF SEPARATE, ADDITIONAL AUTHORIZATION FOR PERSONNEL DECISIONS.—A health information person subject to section 122 may not disclose personal health information to any employees or agents who are responsible for making employment, work assignment, or other personnel decisions with respect to the subject of the information without a separate, additional written authorization permitting such a disclosure.

(e) REQUIREMENT OF SEPARATE, ADDITIONAL AUTHORIZATION FOR MARKETING.—

(1) IN GENERAL.—A health information person may not disclose personal health information for marketing purposes without a separate, additional written authorization permitting such a disclosure.

(2) REQUIREMENTS.—In the case of a disclosure of personal health information for marketing purposes, a separate authorization required by paragraph (1), to be valid, shall—

(A) state that one purpose of the disclosure is for ''marketing'';

(B) state that the purpose of the use or disclosure involved is marketing;

(C) describe the specific marketing uses and disclosures authorized, including whether the personal health information involved—

(i) may be used for purposes internal to the person;

(ii) may be disclosed to, and used by, a business associate of the person; and

(iii) may be disclosed to, and used by, any person or entity other than a business associate of the person; and

(D) state that the use or disclosure of personal health information for marketing will directly result in remuneration to the person from a third party, in any case in which a person expects, or reasonably should expect, that such remuneration will occur.

(3) MARKETING DEFINED.—

(A) IN GENERAL.—In this subsection, the term ''marketing'' is a communication about a product or service a purpose of which is to encourage recipients of the communication to pur-

chase or use the product or service in return for direct or indirect compensation.

(B) EXCLUSIONS.—

(i) IN GENERAL.—Subject to clause (ii), such term excludes the following exceptions:

(I) Communications made by person for the purpose of describing the entities participating in a provider network or health plan network, and communications made by a person for the purpose of describing if and the extent to which a product or service, or payment for a product or service, is provided by the person or included in a benefit plan.

(II) Communications tailored to the circumstances of a particular individual, made by a health care provider to an individual as part of the treatment of the individual, and for the purpose of furthering the treatment of that individual.

(III) Communications tailored to the circumstances of a particular indi-

vidual and made by a health care provider or health plan to an individual in the course of managing or coordinating the treatment of that individual or for the purpose of directing or recommending to that individual alternative treatments, therapies, providers, or settings of care.

(ii) EXCEPTION.—Clause (i) shall not apply, and a communication shall be considered marketing, if a person receives direct or indirect remuneration from a third party for making a written communication otherwise described in subclause (I), (II), or (III) of such clause.

(f) REQUIREMENT TO RELEASE PERSONAL HEALTH INFORMATION TO CORONERS AND MEDICAL EXAMINERS.—

(1) IN GENERAL.—When a coroner or medical examiner or their duly appointed deputies seek personal health information for the purpose of inquiry into and determination of, the cause, manner, and circumstances of an individual's death, the health information person shall provide that individual's personal health information to the coroner or medical

examiner or to the duly appointed deputies without undue delay or consent by the deceased individual's representative.

(2) PRODUCTION OF ADDITIONAL INFORMATION.—If a coroner or medical examiner or their duly appointed deputies receives health information from a person referred to in paragraph (1), such health information shall remain as personal health information unless the health information is attached to or otherwise made a part of a coroner's or medical examiner's official report, in which case it shall no longer be protected.

(3) EXEMPTION.—Health information attached to or otherwise made a part of a coroner's or medical examiner's official report shall be exempt from the provisions of this title except as provided for in this subsection.

(4) REIMBURSEMENT.—A person referred to in paragraph (1) may request reimbursement from a coroner or medical examiner for the reasonable costs associated with inspection or copying of personal health information maintained, retained, or stored by such person.

(g) REVOCATION OR AMENDMENT OF CONSENT OR AUTHORIZATION.—An individual may revoke or amend in

writing an informed consent or authorization under this section at any time.

(h) ACTIONS.—It shall not be a violation of this title with respect to the disclosure of personal health information—

(1) if the disclosure was made based on a good faith reliance on the individual's informed consent or authorization under this section at the time disclosure was made;

(2) in a case in which the consent or authorization is revoked, if the disclosing person had no actual or constructive notice of the revocation; or

(3) if the disclosure was for the purpose of protecting another individual from imminent physical harm and is authorized under section 141.

(i) RECORD OF CONSENTS, AUTHORIZATIONS, AND REVOCATIONS.—Each person accessing, maintaining, retaining, modifying, recording, storing, destroying, or otherwise using personally identifiable or personal health information for purposes other than treatment or payment shall maintain a record for a period of 6 years of each informed consent and authorization by an individual and any revocation thereof, and such record shall become part of the individual's health record set.

CHAPTER 2—EXCEPTIONS

SEC. 131. DISCLOSURE FOR LAW ENFORCEMENT, NATIONAL SECURITY, AND INTELLIGENCE PURPOSES.

(a) ACCESS TO PERSONAL HEALTH INFORMATION FOR LAW ENFORCEMENT, NATIONAL SECURITY, AND INTELLIGENCE ACTIVITIES.—A health information person, or a person who receives personal health information pursuant to section 131, may disclose personal health information to—

(1) an investigative or law enforcement officer (as defined in subsection (k)) pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, civil subpoena, civil investigative demand, or a court order under limitations set forth in subsection (b); and

(2) an authorized Federal official for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401 et seq.) and implementing authority (Executive Order 12333), or otherwise by law.

(b) LIMITATION ON USE AND DISCLOSURE FOR NATIONAL SECURITY, INTELLIGENCE, AND OTHER LAW ENFORCEMENT INQUIRIES.—

(1) IN GENERAL.—Personal health information about an individual that is disclosed under this section may not be used in, or disclosed to any entity for use in, any administrative, civil, or criminal action or investigation directed against the individual, unless the action or investigation arises out of, or is directly related to, the law enforcement, national security, or intelligence inquiry for which the information was obtained.

(2) LAW ENFORCEMENT INQUIRY DEFINED.—In paragraph (1), the term ''law enforcement inquiry'' means a lawful executive branch investigation or official proceeding inquiring into a violation of, or failure to comply with, any criminal or civil statute or any regulation, rule, or order issued pursuant to such a statute.

(c) REDACTIONS.—To the maximum extent practicable, and consistent with the requirements of due process, a law enforcement agency shall redact personally identifying information from personal health information prior to the public disclosure of such protected information in a judicial or administrative proceeding.

(d) EXCEPTION.—This section shall not be construed to limit or restrict the ability of law enforcement authorities to gain information while in hot pursuit of a suspect or if other exigent circumstances exist.

(e) INVESTIGATIVE OR LAW ENFORCEMENT OFFICER DEFINED.—In this section, the term ''investigative or law enforcement officer'' means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of, or to make arrests for, civil or criminal offenses, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses.

SEC. 132. DISCLOSURE FOR PUBLIC HEALTH PURPOSES.

(a) IN GENERAL.—A health information person may disclose personal health information to a public health authority (as defined in section 171(24)) or other entity authorized by public health law, when receipt of such information by the authority or other entity—

(1) relates directly to a specified public health purpose;

(2) is reasonably likely to achieve such purpose; and

(3) is intended for a purpose that cannot be achieved through the receipt or use of de-identified health information.

(b) PUBLIC HEALTH PROTECTION DEFINED.—For purposes of subsection (a), the term ''public health purpose'' means a population-based activity or individual effort, authorized by law, the purpose of which is the prevention of injury, disease, or premature mortality, or the promotion of health, in a community, including—

(1) assessing the health needs and status of the community through public health surveillance and epidemiological research;

(2) implementing public health policy;

(3) responding to public health needs and emergencies; and

(4) any other activities or efforts authorized by law.

(c) LIMITATIONS.—The purpose of the disclosure described in subsection (a) shall be of significant importance such that it warrants the potential effect on, or risk to, the privacy of individuals that the additional exposure of personal health information might bring. Any infringement on the right to privacy under this section shall use the least intrusive means that are tailored to minimize intrusion on the right to privacy.

SEC. 133. REPORTING OF ABUSE AND NEGLECT TO PROTECTION AND ADVOCACY AGENCIES.

Any health information person may disclose personal health information to a protection and advocacy agency established under part C of title I of the Developmental Disabilities Assistance and Bill of Rights Act (42 U.S.C. 6041 et seq.) or under the Protection and Advocacy for Mentally Ill Individuals Act of 1986 (42 U.S.C. 10801 et seq.) when such person reasonably believes that an individual who is the subject of the personal health information is vulnerable to abuse and neglect by an entity providing health or social services to the individual.

SEC. 134. DISCLOSURE TO NEXT OF KIN AND DIRECTORY INFORMATION.

(a) NEXT OF KIN.—A health care provider, or a person that receives personal health information under section 141, may disclose personal health information about health care services provided to an individual to the individual's next of kin, or to another entity that the individual has identified, if at the time of the treatment of the individual—

(1) the individual—

(A) has been notified of the individual's right to object to such disclosure and the individual has not objected to the disclosure; or

(B) is in a physical or mental condition such that the individual is not capable of objecting, and there are no prior indications that the individual would object; and

(2) the information disclosed is relevant to health care services currently being provided to that individual.

(b) DIRECTORY INFORMATION.—

(1) DISCLOSURE.—

(A) IN GENERAL.—Except as provided in paragraph (2), with respect to an individual who is admitted as an inpatient to a health care facility, a person described in subsection (a) may disclose information described in subparagraph (B) about the individual to any entity if, at the time of the admission, the individual—

(i) has been notified of the individual's right to object and has not objected to the disclosure; or

(ii) is in a physical or mental condition such that the individual is not capable of objecting and there are no prior indications that the individual would object.

(B) INFORMATION.—Information described in this subparagraph is information that consists only of 1 or more of the following items:

(i) The name of the individual who is the subject of the information.

(ii) The general health status of the individual, described as critical, poor, fair, stable, or satisfactory or in terms denoting similar conditions.

(iii) The location of the individual within the health care facility to which the individual is admitted.

(2) EXCEPTION.—Paragraph (1)(B)(iii) shall not apply if disclosure of the location of the individual would reveal specific information about the physical or mental condition of the individual, unless the individual expressly authorizes such disclosure.

(c) DIRECTORY OR NEXT-OF-KIN INFORMATION.—A disclosure may not be made under this section if the disclosing person described in subsection (a) has reason to believe that the disclosure of directory or next-of-kin information could lead to the physical or mental harm of the individual, unless the individual expressly authorizes such disclosure.

CHAPTER 3—SPECIAL CIRCUMSTANCES

SEC. 141. EMERGENCY CIRCUMSTANCES.

(a) GENERAL RULE.—In the event of a threat of imminent physical or mental harm to the subject of personal health information, any person may, in order to allay or remedy such threat, disclose personal health information about such subject to a health care provider, health care facility, law enforcement authority, or emergency medical personnel, to the minimum extent necessary and only if determined appropriate by a health care provider.

(b) HARM TO OTHERS.—Any person may disclose personal health information about the subject of the information where—

(1) such subject has made an identifiable threat of serious injury or death with respect to an identifiable individual or group of individuals;

(2) the subject has the ability to carry out such threat; and

(3) the release of such information is necessary to prevent or significantly reduce the possibility of such threat being carried out.

SEC. 142. HEALTH RESEARCH.

(a) REGULATIONS.—

(1) IN GENERAL.—The requirements and protections provided for under part 46 of title 45, Code

of Federal Regulations (as in effect on the date of enactment of this Act), shall apply to all health research.

(2) EFFECTIVE DATE.—Paragraph (1) shall not take effect until the Secretary has promulgated final regulations to implement such paragraph.

(b) EVALUATION.—Not later than 24 months after the date of the enactment of this Act, the Secretary shall prepare and submit to Congress detailed recommendations on whether informed consent should be required, and if so, under what circumstances, before personal health information can be used for health research.

(c) RECOMMENDATIONS.—The recommendations required to be submitted under subsection (b) shall include—

(1) a detailed explanation of current institutional review board practices, including the extent to which the privacy of individuals is taken into account as a factor before allowing waivers and under what circumstances informed consent is being waived;

(2) a list of all known breaches of health information privacy over the past 5 years in research projects approved by an institutional review board;

(3) a summary of how technology that both facilitates research and preserves privacy could be used to obtain informed consent and strip identifying data for the purpose of research;

(4) an analysis of State and Federal laws, medical ethics, and ethics in the performance of health research that examines requirements for the receipt of informed consent; and

(5) an analysis of the risks and benefits of allowing individuals to consent or to refuse to consent, at the time of receiving medical treatment, to the possible future use of records of medical treatments for research studies.

(d) CONSULTATION.—In carrying out this section, the Secretary shall consult with individuals who have distinguished themselves in the fields of health research, privacy, related technology including electronic consent management tools, consumer interests in health information, health data standards, and the provision of health services.

(e) CONGRESSIONAL NOTICE.—Not later than 6 months after the date on which the Secretary submits to Congress the recommendations required under subsection (b), the Secretary shall propose to implement such recommendations through regulations promulgated on the

record after opportunity for a hearing, and shall advise the Congress of such proposal.

(f) OTHER REQUIREMENTS.—

(1) OBLIGATIONS OF THE RECIPIENT.—A person who receives personal health information pursuant to this section shall remove or destroy, at the earliest opportunity consistent with the purposes of the project involved, information that would enable an individual to be identified, unless—

(A) an institutional review board has determined that there is a health or research justification for the retention of such identifiers;

(B) an institutional review board has, to the maximum extent practicable, attempted to contact the individual to whom the identifiers relate;

(C) upon being contacted pursuant to subparagraph (B), the individual does not object to the retention of such identifiers; and

(D) there is an adequate plan to protect the identifiers from disclosure consistent with this section.

(2) PERIODIC REVIEW AND TECHNICAL ASSISTANCE.—

(A) INSTITUTIONAL REVIEW BOARD.—Any institutional review board that authorizes research under this section shall provide the Secretary with the names and addresses of the institutional review board members.

(B) TECHNICAL ASSISTANCE.—The Secretary shall provide technical assistance to institutional review boards described in this subsection.

(C) MONITORING.—The Secretary shall periodically monitor institutional review boards described in this subsection, including with respect to the privacy, security, and confidentiality practices of such boards.

(D) REPORTS.—Not later than 3 years after the date of enactment of this Act, the Secretary shall report to Congress regarding the activities of institutional review boards described in this subsection.

(g) LIMITATION.—Nothing in this section shall be construed to permit personal health information that is received by a researcher under this section to be accessed for purposes other than research or as authorized by the individual that is the subject of such personal health information.

SEC. 143. HEALTH OVERSIGHT FUNCTIONS.

(a) IN GENERAL.—A health information person may disclose personal health information to a health oversight agency (as defined in section 171(16)) to enable the agency to perform a health oversight function authorized by law, if—

(1) the purpose for which the disclosure is to be made cannot reasonably be accomplished without personal health information;

(2) the purpose for which the disclosure is to be made is of sufficient importance to warrant the effect on, or the risk to, the privacy of the individuals that additional exposure of the information might bring; and

(3) there is a reasonable probability that the purpose of the disclosure will be accomplished.

(b) USE AND MAINTENANCE OF PERSONAL HEALTH INFORMATION.—A health oversight agency that receives personal health information under subsection (a)—

(1) shall, to the maximum extent practicable, obtain the informed consent of the individual to whom the personal health information relates before using or disclosing the information;

(2) shall secure personal health information in all work papers and all documents summarizing the health oversight activity through technological, ad-

ministrative, and physical safeguards including cryptographic-key based encryption;

(3) shall maintain in its records only such information about an individual as is relevant and necessary to accomplish the purpose for which the personal health information was obtained;

(4) using appropriate encryption measures, shall maintain such information securely and limit access to such information to those persons with a legitimate need for access to carry out the purpose for which the records were obtained; and

(5) shall remove or destroy the information that allows subjects of personal health information to be identified at the earliest time at which removal or destruction can be accomplished, consistent with the purpose of the health oversight activity.

(c) AUTHORIZATION BY A SUPERVISOR.—For purposes of this section, the individual with authority to authorize the oversight function involved shall provide to the disclosing person described in subsection (a) a statement that the personal health information is being sought for a legally authorized oversight function.

SEC. 144. INDIVIDUAL REPRESENTATIVES.

(a) IN GENERAL.—Except as provided in subsections (b) and (c), a person who is authorized by law (based on

grounds other than an individual's status as a minor), or by an instrument recognized under law, to act as an agent, attorney, proxy, or other legal representative of an individual, may, to the extent so authorized, exercise and discharge the rights of the individual under this title.

(b) HEALTH CARE POWER OF ATTORNEY.—A person who is authorized by law (based on grounds other than being a minor), or by an instrument recognized under law, to make decisions about the provision of health care to an individual who is incapacitated, may exercise and discharge the rights of the individual under this title to the extent necessary to effectuate the terms or purposes of the grant of authority.

(c) INDIVIDUALS SUFFERING FROM CERTAIN MEDICAL CONDITIONS.—If a physician or other health care provider determines that an individual, who has not been declared to be legally incompetent, suffers from a medical condition that prevents the individual from acting knowingly or effectively on the individual's own behalf, the right of the individual to access or amend the health information and to authorize disclosure under this title may be exercised and discharged in the best interest of the individual by—

(1) a person described in subsection (b) with respect to the individual;

(2) a person described in subsection (a) with respect to the individual, but only if a person described in paragraph (1) cannot be contacted after a reasonable effort or if there is no individual who fits the description in paragraph (1);

(3) the next of kin of the individual, but only if a person described in paragraph (1) or (2) cannot be contacted after a reasonable effort; or

(4) the health care provider, but only if a person described in paragraph (1), (2), or (3) cannot be contacted after a reasonable effort.

(d) RIGHTS OF MINORS.—

(1) INDIVIDUALS WHO ARE 18 OR LEGALLY CAPABLE.—In the case of an individual—

(A) who is 18 years of age or older, all rights of the individual under this title shall be exercised by the individual; or

(B) who, acting alone, can consent to health care without violating any applicable law, and who has sought such care, the individual shall exercise all rights of an individual under this title with respect to personal health information relating to such health care.

(2) INDIVIDUALS UNDER 18.—Except as provided in paragraph (1)(B), in the case of an individual who is—

(A) under 14 years of age, all of the individual's rights under this title shall be exercised through the parent or legal guardian; or

(B) 14 through 17 years of age, the rights of inspection, supplementation, and modification, and the right to authorize use and disclosure of personal health information of the individual shall be exercised by—

(i) the individual where no parent or legal guardian exists;

(ii) the parent or legal guardian of the individual; or

(iii) the individual if the parent or legal guardian determined that the individual has the sole right the control their health information.

(e) DECEASED INDIVIDUALS.—

(1) APPLICATION OF ACT.—The provisions of this title shall continue to apply to personal health information concerning a deceased individual.

(2) EXERCISE OF RIGHTS ON BEHALF OF A DECEASED INDIVIDUAL.—A person who is authorized

by law or by an instrument recognized under law, to act as an executor or administrator of the estate of a deceased individual, or otherwise to exercise the rights of the deceased individual, may, to the extent so authorized, exercise and discharge the rights of such deceased individual under this title. If no such designee has been authorized, the rights of the deceased individual may be exercised as provided for in subsection (c).

(3) IDENTIFICATION OF DECEASED INDIVIDUAL.—A person described in section 136(a) may disclose personal health information if such disclosure is necessary to assist in the identification of a deceased individual.

Subtitle D—Enforcement

SEC. 151. IN GENERAL.

(a) CIVIL PENALTY.—A health information person who the Secretary, in consultation with the Attorney General, determines has substantially and materially failed to comply with this title shall be subject, in addition to any other penalties that may be prescribed by law—

(1) in a case in which the violation relates to subtitle A, B, or C, to a civil penalty of not more than $500 for each such violation, but not to exceed $5,000 in the aggregate for multiple violations;

(2) in a case in which the violation relates to subtitle A, B, or C, to a civil penalty of not more than $10,000 for each such violation, but not to exceed $50,000 in the aggregate for multiple violations; or

(3) in a case in which such violations have occurred with such frequency as to constitute a general business practice, to a civil penalty of not more than $100,000.

(b) CIVIL ACTION BY INDIVIDUALS.—

(1) IN GENERAL.—Any individual whose rights under subtitle A, B, or C have been knowingly or negligently violated may bring a civil action to recover—

(A) such preliminary and equitable relief as the court determines to be appropriate; and

(B) the greater of compensatory damages or liquidated damages of $5,000.

(2) ADDITIONAL REMEDIES.—The equitable relief or damages that may be available under this section shall be in addition to any other lawful remedy or award that may be available.

SEC. 152. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) CIVIL ACTIONS.—In any case in which the attorney general of a State or any State or local law enforce-

ment agency authorized by the State attorney general or by State law to prosecute violations of consumer protection laws, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of a person in a practice that is prohibited under subtitle A, B, or C, the State or local law enforcement agency on behalf of the residents of the agency's jurisdiction, may bring a civil action on behalf of the residents of the State or jurisdiction in a district court of the United States of appropriate jurisdiction to—

(1) enjoin that act or practice;

(2) enforce compliance with the respective subtitle; or

(3) obtain civil penalties in an amount calculated by multiplying the number of violations by an amount not greater than $11,000.

For purposes of civil penalties under this subsection, each day that a person is in violation of the requirements of subtitle A, B, or C shall be treated as a separate violation, up to a maximum civil penalty of $5,000,000.

(b) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this subtitle regarding notification shall be construed to prevent an attorney general of a State from exercising the

powers conferred on such attorney general by the laws of that State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

(3) compel the attendance of witnesses or the production of documentary and other evidence.

(c) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(2) SERVICE OF PROCESS.—In an action brought under subsection (a), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

Subtitle E—Miscellaneous

SEC. 161. OFFICE OF HEALTH INFORMATION PRIVACY.

(a) IN GENERAL.—The Secretary shall designate an office within the Department of Health and Human Services to be known as the Office of Health Information Privacy (referred to in this section as the ''Office''). The Office shall be headed by a Director, who shall be appointed by the Secretary.

(b) DUTIES.—The Director of the Office shall—

(1) receive and investigate complaints of alleged violations of this title;

(2) provide for the conduct of audits where appropriate;

(3) provide guidance to the Secretary on the implementation of this Act;

(4) provide guidance to health care providers and other relevant individuals concerning the manner in which to interpret and implement the privacy protections under this title (and the regulations promulgated under this title);

(5) prepare and submit the report described in subsection (c);

(6) consult with, and provide recommendation to, the Secretary concerning improvements in the privacy and security of personal health information and concerning medical privacy research needs; and

(7) carry out any other activities determined appropriate by the Secretary.

(c) STANDARDS FOR CERTIFICATION.—

(1) ESTABLISHMENT.—Not later than 12 months after the date of enactment of this Act, the Secretary, in consultation with the Director of the Office and the Director of the Office of Civil Rights,

shall establish and implement standards for health information technology products, including qualified health information technology systems (as defined in section 213), used to access, disclose, maintain, store, distribute, transmit, amend, or dispose of personal health information in a manner that protects the individual's right to privacy, confidentiality, and security relating to that information.

(2) STAKEHOLDER PARTICIPATION.—In establishing the standards under paragraph (1), the Secretary shall ensure the participation of various stakeholders, including patients and consumer advocates, privacy advocates, experts in information technology and information systems, and experts in health care. The Secretary shall ensure that these advocates and experts are equally represented, such that the stakeholder process does not result in the experts in information technology, information systems, and health care being disproportionately represented compared to advocates for the interests of consumers and privacy proponents.

(d) REPORT ON COMPLIANCE.—Not later than January 1 of the first calendar year beginning more than 1 year after the establishment of the Office under subsection (a), and every January 1 thereafter, the Secretary, in con-

sultation with the Director of the Office, shall prepare and submit to Congress a report concerning the number of complaints of alleged violations of subtitle A that are received during the year for which the report is being prepared. Such report shall describe the complaints and any remedial action taken concerning such complaints and shall be made available to the public on the Internet website of the Department of Health and Human Services.

SEC. 162. PROTECTION FOR WHISTLEBLOWERS.

(a) PROHIBITION AGAINST DISCRIMINATION.—A health information person may not—

(1) discharge, demote, suspend, threaten, harass, retaliate against, or in any other manner discriminate or cause any employer to discriminate against an employee in the terms and conditions of employment because of—

(A) the refusal of the employee to engage in a violation of this title; or

(B) any lawful act the employee has committed or is about to commit, or which the health information person perceives the employee to have committed, to provide information or cause information to be provided, including in the course of the employee's routine job duties, to the individual's employer or to a

State or Federal official relating to an actual or suspected violation of this title by any person, including an employer or an employee of an employer; or

(2) adversely affect another person, directly or indirectly, because such person has exercised a right under this title, disclosed information relating to a possible violation of subtitle A, B, or C or this section, or associated with, or assisted, an individual in the exercise of a right under this title

(b) ENFORCEMENT ACTIONS.—

(1) IN GENERAL.—

(A) COMPLAINT WITH SECRETARY OF LABOR.—Any employee or former employee who alleges a violation of subsection (a) may seek relief under subsection (c), by filing a complaint with the Secretary of Labor.

(B) APPELLATE REVIEW IN CASE OF FINAL ORDER.—Unless an employee brings an action in district court under subparagraph (C), any person adversely affected or aggrieved by a final order of the Secretary of Labor with respect to a complaint filed under subparagraph (A) may obtain review of the order in the United States court of appeals for the circuit in

which the violation, with respect to which the order was issued, allegedly occurred or the circuit in which the complainant resided on the date of such violation. The petition for review must be filed not later than 60 days after the date of the issuance of the final order. The review shall conform to chapter 7 of title 5, United States Code. The commencement of proceedings under this subparagraph shall not, unless ordered by the court, operate as a stay of the order.

(C) DE NOVO REVIEW.—If the Secretary of Labor has not issued a final decision within 180 days after the filing of the complaint, or within 90 days after receiving any written determination, the complainant may bring an action at law or equity for de novo review in the appropriate district court of the United States with jurisdiction, which shall have jurisdiction over such an action without regard to the amount in controversy, and which action shall, at the request of either party to such action, be tried by the court with a jury.

(2) PROCEDURES.—

(A) IN GENERAL.—Except as provided in this paragraph, the complaint procedures contained in section 42121(b) of title 49, United States Code, shall apply with respect to a complaint filed under paragraph (1)(A).

(B) EXCEPTION.—With respect to a complaint filed under paragraph (1)(A), the notification provided for under section 42121(b)(1) of title 49, United States Code, (as required under subparagraph (A)) shall be made to the person named in the complaint and to the employer.

(C) BURDEN OF PROOF.—The legal burdens of proof contained in section 42121(b) of title 49, United States Code, shall apply to any action brought under this subsection.

(D) STATUTE OF LIMITATIONS.—A complaint shall be filed under paragraph (1)(A) not later than 2 years after the date on which the alleged violation occurs.

(E) CIVIL ACTIONS TO ENFORCE.—If a person fails to comply with an order issued by the Secretary of Labor pursuant to the procedures in section 42121(b) of title 49, United States Code, the Secretary shall have the au-

thority described in section 42121(b)(5) of title 49, United States Code, to bring a civil action to enforce the order in the district court of the United States for the judicial district in which the violation occurred.

(c) REMEDIES.—

(1) IN GENERAL.—If the Secretary of Labor or the district court determines that a violation of subsection (a) has occurred, the Secretary or court shall order any relief necessary to make the employee whole.

(2) COMPENSATORY DAMAGES.—Relief in any action under such subsection shall include—

(A) reinstatement of the employee to the employee's former position with the same seniority status that the employee would have had but for the discrimination;

(B) payment of the amount of back pay, with interest, to which the employee is entitled; and

(C) the payment of compensation for any special damages sustained by the employee as a result of the discrimination, including litigation costs, expert witness fees, and reasonable attorney fees.

(3) PUNITIVE DAMAGES.—Relief in any action under such subsection may include punitive damages in an amount not to exceed $250,000.

(d) RIGHTS RETAINED BY THE EMPLOYEE.—Nothing in this section shall be construed to diminish or eliminate the rights, privileges, or remedies available to an employee under any Federal or State law, or under any collective bargaining agreement.

(e) LIMITATION.—The protections of this section shall not apply to any employee who—

(1) deliberately causes or participates in the alleged violation; or

(2) knowingly or recklessly provides materially false information to an individual or entity described in subsection (a).

(f) DEFINITIONS.—In this section:

(1) EMPLOY.—The term ''employ'' has the meaning given such term under section 3(g) of the Fair Labor Standards Act of 1938 (29 U.S.C. 203(g)) for the purposes of implementing the requirements of that Act (29 U.S.C. 201, et seq.).

(2) EMPLOYEE.—The term ''employee'' means an individual who is employed by an employer.

(3) EMPLOYER.—The term ''employer'' means any person who employs employees, including any

person acting directly or indirectly in the interest of any employer in relation to an employee and includes a public agency.

SEC. 163. DEMONSTRATION GRANT FOR INDIVIDUALS WITH LIMITED ENGLISH LANGUAGE PROFICIENCY OR LIMITED HEALTH LITERACY.

(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 personal health information, and to enable such persons to better communicate privacy procedures 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. 164. RELATIONSHIP TO OTHER LAWS.

(a) FEDERAL AND STATE LAWS.—Nothing in this Act shall be construed as preempting, superseding, or repealing, explicitly or implicitly, other Federal or State laws or regulations relating to personal health information or relating to an individual's access to personal health information or health care services, if such laws or regulations provide protections for the rights of individuals to the privacy of, and access to, their health information that is greater than those provided for in this Act.

(b) PRIVILEGES.—Nothing in this Act shall be construed to preempt or modify any provisions of State statutory or common law to the extent that such law concerns a privilege of a witness or person in a court of that State. This Act shall not be construed to supersede or modify any provision of Federal statutory or common law to the extent such law concerns a privilege of a witness or entity prior to a court proceeding or in a court of the United States. Informed consent shall not be construed as a waiver of any such privilege.

(c) CERTAIN DUTIES UNDER LAW.—Nothing in this Act shall be construed to preempt, supersede, or modify the operation of any State law that—

(1) provides for the reporting of vital statistics such as birth or death information;

(2) requires the reporting of abuse or neglect information about any individual;

(3) regulates the disclosure or reporting of information concerning an individual's mental health; or

(4) governs a minor's rights to access personal health information or health care services.

(d) HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT.—The standards governing the privacy and security of individually identifiable health information promulgated by the Secretary of Health and Human Services under sections 262(a) and 264 of the Health Insurance Portability and Accountability Act of 1996 shall remain in effect to the extent that they are consistent with this title. The Secretary shall by rule amend such Federal regulations as required to make such regulations consistent with this title.

SEC. 165. EFFECTIVE DATE.

(a) EFFECTIVE DATE.—Unless specifically provided for otherwise, this title shall take effect on the date that is 12 months after the date of the promulgation of the regulations required under subsection (b), or 30 months after the date of enactment of this Act, whichever is earlier.

(b) REGULATIONS.—Not later than 12 months after the date of enactment of this Act, or as specifically provided for otherwise, the Secretary shall promulgate regulations implementing this title.

Subtitle F—General Definitions

SEC. 171. GENERAL DEFINITIONS.

In this Act:

(1) AGENT.—The term ''agent'' means a person that represents or acts for another person (a principal) under a contract or relationship of agency, or that functions to bring about, modify, affect, accept performance of, or terminate, contractual obligations between the principal and a third person. With respect to an employer, such term includes the employees of the employer.

(2) AUTHORIZATION.—The term ''authorization'' means the authority granted by an individual that is the subject of personal health information, in accordance with this title, for the disclosure or use of the individual's personal health information.

(3) BREACH.—The term ''breach'' means the unauthorized acquisition, disclosure, or loss of personal health information which compromises the security, privacy, or integrity of personal health information maintained by or on behalf of a person.

(4) CONFIDENTIALITY.—The term ''confidentiality'' means the obligations of those who receive information to respect the privacy interests of those to whom the data relate.

(5) DE-IDENTIFIED HEALTH INFORMATION.—The term ''de-identified health information'' means any personal health information, with respect to which—

(A) all personal identifiers, or other information that may be used by itself or in combination with other information which may be available to re-identify (as defined in section 171(25)) the subject of the information (such as geographic, credit, and financial information and all of the identifiers enumerated at section 164.514(b)(2) of title 45 of the Code of Federal Regulations (as in effect on January 1, 2008)) have been removed;

(B) a good faith effort has been made to evaluate, minimize, and mitigate the risks of re-identification of the subject of such information, using commonly accepted scientific and statistical standards and methods for minimizing risk of disclosure; and

(C) there is no reasonable basis to believe that the information can be used to identify an individual.

(6) DISCLOSE.—The term ''disclose'' means to release, publish, share, transfer, transmit, disseminate, show, permit access to, communicate (orally or otherwise), re-identify, or otherwise divulge personal health information to any person other than the individual who is the subject of such information. Such term includes the initial disclosure and any subsequent re-disclosure of personal health information.

(7) DECRYPTION KEY.—The term ''decryption key'' means the variable information used in or produced by a mathematical formula, code, or algorithm, or any component thereof, used for encryption (as defined in paragraph (10)) or decryption of wire, electronic, or other communications or stored information.

(8) DIRECTOR OF THE OFFICE OF HEALTH INFORMATION PRIVACY.—The term ''Director of the Office of Health Information Privacy'' means such Director as appointed under section 161.

(9) EMPLOYER.—Except as otherwise provided in section 164, the term ''employer'' means a person

that is engaged in business affecting commerce and that has employees.

(10) ENCRYPTION.—The term ''encryption''—

(A) means the protection of data in electronic form, in storage or in transit, using an encryption technology that has been adopted by an established standards setting body which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and

(B) includes appropriate management and safeguards of such cryptographic keys so as to protect the integrity of the encryption.

(11) HEALTH CARE.—The term ''health care'' means—

(A) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, including appropriate assistance with disease or symptom management and maintenance, counseling, service, or procedure—

(i) with respect to the physical or mental condition of an individual; or

(ii) affecting the structure or function of the human body or any part of the human body, including the banking of

blood, sperm, organs, or any other tissue; or

(B) any sale or dispensing of a drug, device, equipment, or other health care-related item to an individual, or for the use of an individual, pursuant to a prescription.

(12) HEALTH CARE PROVIDER.—The term ''health care provider'' means a person that, with respect to a specific item of personal health information, receives, accesses, maintains, retains, modifies, records, stores, destroys, or otherwise uses or discloses the information while acting in whole or in part in the capacity of—

(A) an entity that is, or holds itself out to be, licensed, certified, registered, or otherwise authorized by Federal or State law to provide an item or service that constitutes health care in the ordinary course of business, or practice of a profession;

(B) a contractor or other health care provider or facility authorized to provide items or services related to diagnosis or treatment of a health concern, including a hospital, nursing facility, allied health professional, and a facility

used or maintained by allied health professionals;

(C) a Federal or State program that directly provides items or services that constitute health care to beneficiaries;

(D) an officer or employee or agent of a person described in subparagraph (A) or (C) who is engaged in the provision of health care or who uses personal health information; or

(E) medical personnel in an emergency situation, including while communicating personal health information by radio transmission or other means.

(13) HEALTH INFORMATION PERSON.—The term ''health information person'' means, in relation to personal health information, a person, including a health care provider, health researcher, health plan, health insurer, health care clearinghouse, health oversight agency, or public health authority, or such person's agent, officer, employee, or affiliate, that accesses, maintains, retains, modifies, records, stores, or otherwise holds, uses, or discloses such information.

(14) HEALTH PLAN.—

(A) IN GENERAL.—The term ''health plan'' means—

(i) a group health plan (as defined in section 2791(a)(1) of the Public Health Service Act (42 U.S.C. 300gg–91(a)(1)));

(ii) health insurance coverage (as such term is defined in section 2791(b)(1) of the Public Health Service Act (42 U.S.C. 300gg–91(b)(1)); or

(iii) a safety net health plan (as defined in subparagraph (B)).

(B) SAFETY NET HEALTH PLAN.—For purposes of subparagraph (A)(iii), the term ''safety net health plan'' means a managed care organization, as defined in section 1932(a)(1)(B)(i) of the Social Security Act—

(i) that is exempt from or not subject to Federal income tax, or that is owned by an entity or entities exempt from or not subject to Federal income tax; and

(ii) for which not less than 75 percent of the enrolled population receives benefits under a Federal health care program (as defined in section 1128B(f)(1) of the Social Security Act) or a health care plan or

program which is funded, in whole or in part, by a State (other than a program for government employees).

(15) HEALTH OR LIFE INSURER.—The term ''health or life insurer'' means a health insurance issuer (as defined in section 9805(b)(2) of the Internal Revenue Code of 1986) or a life insurance company (as defined in section 816 of such Code) and includes the employees and agents of such a person.

(16) HEALTH OVERSIGHT AGENCY.—The term ''health oversight agency''—

(A) means a person that—

(i) performs or oversees the performance of an assessment, investigation, or prosecution relating to compliance with legal or fiscal standards relating to health care fraud or fraudulent claims regarding health care, health services or equipment, related activities and items, or the effectiveness of health privacy and security measures; and

(ii) is a public executive branch agency, acting on behalf of a public executive branch agency, acting pursuant to a requirement of a public executive branch

agency, or carrying out activities under a Federal or State law governing an assessment, evaluation, determination, investigation, or prosecution described in clause (i); and

(B) includes the employees and agents of such a person.

(17) HEALTH RECORD SET.—The term ''health record set'' means any item, collection, or grouping of information that includes personal health information, such as a medical record, electronic health record, electronic medical record, personal health record, or account of disclosure, use or access, that is created, accessed, received, maintained, retained, modified, recorded, stored, destroyed, or otherwise used or disclosed by a health care provider, employer, insurer, health plan, health researcher, data partner, or other person that relates to the health or illness of the body, mind, or genome of an individual.

(18) HEALTH RESEARCHER.—The term ''health researcher'' means a person that is engaged in activities conducted for the purpose of advancing public knowledge and, with respect to a specific item of

personal health information, receives the information—

(A) pursuant to section 142 (relating to health research); or

(B) while acting in whole or in part in the capacity of an officer, employee, or agent of a person that receives the information pursuant to such section.

(19) INFORMED CONSENT.—

(A) IN GENERAL.—Subject to subparagraph (B), the term ''informed consent'' means the written authorization for use or disclosure of personal health information by the individual who is the subject of such information, conditioned upon—

(i) that individual's having been informed of the nature and probability of harm to the individual resulting from such authorization; and

(ii) the authorization meeting the requirements of section 122(b).

(B) THROUGH INFERENCE.—Informed consent may be inferred, in the absence of a contrary indication by the individual—

(i) to the extent necessary to provide treatment and obtain payment for health care in emergency situations;

(ii) to the extent necessary to provide treatment and payment where a health care provider is required by law to treat the individual;

(iii) if the health care provider is unable to obtain informed consent due to substantial barriers to communicating with the individual and the provider reasonably infers from the circumstances, based upon the exercise of professional judgment, that the individual does not object to the disclosure or the disclosure is in the best interest of the individual; and

(iv) to the extent the information is necessary to carry out or otherwise implement a medical or mental health practitioner's order or prescription for health services, medical devices or supplies, or pharmaceuticals.

(C) MULTIPLE USES AND DISCLOSURES.—Informed consent may authorize multiple uses or disclosures.

(20) OFFICE OF HEALTH INFORMATION PRIVACY.—The term ''Office of Health Information Privacy'' means the Office of Health Information Privacy designated under section 161.

(21) PERSON.—The term ''person'' means an entity that is a government, governmental subdivision of an executive branch agency or authority, corporation, company, association, firm, partnership, society, estate, trust, joint venture, individual, individual representative, tribal government, or any other legal entity. Such term also includes the employees, contractors, agents, and affiliates of all legal entities described in the preceding sentence, whether or not they are acting in the capacity of their employment, contract, agency, or affiliation.

(22) PRIVACY.—The term ''privacy'' means an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data.

(23) PERSONAL HEALTH INFORMATION.—

(A) IN GENERAL.—The term ''personal 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—

(i) is created or received by a health care provider, health researcher, health plan, health or life insurer, medical or health savings plan administrator, health care clearinghouse, health oversight agency, public health authority, employer, data partner, or other person or such person's agent, officer, or employee; and

(ii)(I) 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

(II)(aa) identifies an individual; or

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

(B) INCLUSION OF DECRYPTION KEY.—The term ''personal health information'' includes any decryption key used for the encryption or decryption of information described in subparagraph (A).

(24) PUBLIC HEALTH AUTHORITY.—The term ''public health authority'' means an authority or instrumentality of the United States, a tribal government, a State, or a political subdivision of a State that is—

(A) primarily responsible for public health matters; and

(B) primarily engaged in activities such as injury reporting, public health surveillance, and public health investigation or intervention.

(25) RE-IDENTIFY.—The term ''re-identify'', when used with respect to de-identified health information, means an attempt, successful or otherwise, to ascertain—

(A) the identity of the individual who is the subject of such information; or

(B) the decryption key with respect to the information (when undertaken with knowledge that such key would allow for the identification of the individual who is the subject of such information).

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

(28) SECURITY.—The term ''security'' means physical, technological, or administrative safeguards

or tools used to protect identifiable health data from unwarranted access or disclosure.

(29) SECURITY BREACH.—The term ''security breach'' means the physical, structural, or substantive compromise of the security of personal health information, through unauthorized disclosure, use, or access, whether actual or attempted, resulting in the acquisition, access, or use of such information by an unauthorized person. Such term does not apply to good faith or accidental acquisition, or disclosure of personal health information by an unauthorized person, so long as no further use or disclosure is made by such person.

(30) SEGREGATE.—The term ''segregate'' means to hide, mask, or mark separate a designated subset of an individual's personal health information, or to place such a subset in a location that is securely separated from the location used to store other personal health information, such that access to or use of any information so segregated may be effectively limited to those persons that are authorized by the individual to access or use that segregated information.

(31) SIGNED.—The term ''signed'' refers both to signatures in ink and to electronic signatures that

are authenticated by the individual using an authentication method approved by the Secretary.

(32) STATE.—The term ''State'' means each of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.

(33) TO THE MAXIMUM EXTENT PRACTICABLE.—The term ''to the maximum extent practicable'' means the level of compliance that a reasonable person would deem technologically feasible so long as such feasibility is periodically evaluated in light of scientific advances.

(34) USE.—The term ''use'' means to create, record, collect, access, obtain, store, maintain, amend, correct, restore, modify, supplement, identify, re-identify, employ, apply, utilize, examine, analyze, detect, remove, destroy, dispose of, account for, or monitor the flow of personal health information.

(35) WRITING; WRITTEN.—The terms ''writing'' and ''written'' mean writing or written, respectively, in either a paper-based or computer-based form, including electronic and digital signatures.

TITLE II—PROMOTION OF HEALTH INFORMATION TECHNOLOGY

Subtitle A—Improving the Interoperability of Health Information Technology

SEC. 201. OFFICE OF THE NATIONAL COORDINATOR OF HEALTH INFORMATION TECHNOLOGY.

(a) ESTABLISHMENT.—There is established within the office of the Secretary, the Office of the National Coordinator of Health Information Technology. The National Coordinator shall be appointed by the Secretary in consultation with the President, and shall report directly to the Secretary.

(b) PURPOSE.—The Office of the National Coordinator shall be responsible for—

(1) ensuring that key health information technology initiatives are coordinated across programs of the Department of Health and Human Services;

(2) ensuring that health information technology policies and programs of the Department of Health and Human Services are coordinated with such policies and programs of other relevant Federal agencies (including Federal commissions and advisory committees) with a goal of avoiding duplication of ef-

forts and of helping to ensure that each agency undertakes activities primarily within the areas of its greatest expertise and technical capability;

(3) reviewing Federal health information technology investments to ensure that Federal health information technology programs are meeting the objectives of the strategic plan published by the Office of the National Coordinator of Health Information Technology to establish a nationwide interoperable health information technology infrastructure;

(4) providing comments and advice regarding specific Federal health information technology programs, at the request of Office of Management and Budget;

(5) enhancing the use of health information technology to improve the quality of health care in the prevention and management of chronic disease and to address population health; and

(6) consulting with the Office of Health Information Privacy to ensure that key health information technology initiatives of the Department of Health and Human Services and other Federal agencies are consistent with the privacy, confidentiality, and security requirements in title I.

(c) ROLE WITH AMERICAN HEALTH INFORMATION COMMUNITY AND THE PARTNERSHIP FOR HEALTH CARE IMPROVEMENT.—The Office of the National Coordinator shall—

(1) serve as an ex officio member of the American Health Information Community established under section 203, and act as a liaison between the Federal Government and the Community;

(2) serve as an ex officio member of the Partnership and act as a liaison between the Federal Government and the Partnership for Health Care Improvement (established under section 202); and

(3) serve as a liaison between the Partnership and the Community.

(d) REPORTS AND WEBSITE.—The Office of the National Coordinator shall—

(1) develop and publish a strategic plan for implementing a nationwide interoperable health information technology infrastructure;

(2) maintain and frequently update an Internet website that—

(A) publishes the schedule for the assessment of standards for significant use cases;

(B) publishes the recommendations of the American Health Information Community;

(C) publishes the recommendations of the Partnership for Health Care Improvement;

(D) publishes quality measures;

(E) identifies sources of funds that will be made available to facilitate the purchase of, or enhance the utilization of, health information technology systems, either through grants or technical assistance; and

(F) publishes a plan for a transition of any functions of the Office of the National Coordinator that should be continued after September 30, 2014;

(3) prepare a report on the lessons learned from major public and private health care systems that have implemented health information technology systems, including an explanation of whether the systems and practices developed by such systems may be applicable to and usable in whole or in part by other health care providers; and

(4) assess the impact of health information technology in communities with health disparities and identify practices to increase the adoption of such technology by health care providers in such communities.

(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed as requiring the duplication of Federal efforts with respect to the establishment of the Office of the National Coordinator of Health Information Technology, regardless of whether such efforts are carried out before or after the date of the enactment of this title.

(f) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section, $5,000,000 for each of fiscal years 2009 and 2010.

(g) SUNSET.—The provisions of this section shall not apply after September 30, 2014.

SEC. 202. PARTNERSHIP FOR HEALTH CARE IMPROVEMENT.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—There is established a public-private Partnership for Health Care Improvement (in this title referred to as the ''Partnership'') to—

(A) provide advice to the Secretary and the Nation and recommend specific actions to achieve a nationwide interoperable health information technology infrastructure;

(B) make recommendations concerning standards, including privacy, security, and confidentiality standards, implementation specifications, and certification criteria for the electronic

exchange of personal health information (including for the reporting of quality data under section 221) for adoption by the Federal Government and voluntary adoption by private entities that are consistent with the requirements of title I;

(C) serve as a forum for the participation of a broad range of stakeholders with specific technical expertise in the development of standards, implementation specifications, and certification criteria and protection of privacy and data security to provide input on the effective implementation of health information technology systems; and

(D) develop and maintain an Internet website that—

(i) publishes established governance rules (including a subsequent appointment process);

(ii) publishes a business plan;

(iii) publishes meeting notices at least 14 days prior to each meeting;

(iv) publishes meeting agendas at least 7 days prior to each meeting; and

(v) publishes meeting materials at least 3 days prior to each meeting.

(2) LIMITATION.—The Partnership shall not meet or take any action until an advisory committee charter has been filed with the Secretary and with the appropriate committees of the Senate and House of Representatives for the American Health Information Community described in section 203.

(b) MEMBERSHIP.—

(1) MEMBERS.—The members of the Partnership shall consist of the following:

(A) APPOINTED MEMBERS.—The appointed members of the Partnership shall be appointed as follows:

(i) 2 members shall be appointed by the Secretary.

(ii) 1 member shall be appointed by the majority leader of the Senate.

(iii) 1 member shall be appointed by the minority leader of the Senate.

(iv) 1 member shall be appointed by the Speaker of the House of Representatives.

(v) 1 member shall be appointed by the minority leader of the House of Representatives.

(vi) Seven members shall be appointed by the Comptroller General of whom—

(I) one member shall be a representative of consumer or patient organizations;

(II) one member shall be a representative of organizations with expertise in the protection of privacy;

(III) one member shall be a representative of organizations with expertise in security;

(IV) one member shall be a representative of health care providers;

(V) one member shall be a representative of health plans or other third party payers;

(VI) one member shall be a representative of information technology vendors; and

(VII) one member shall be a representative of purchasers or employers.

(B) NATIONAL COORDINATOR.—The National Coordinator shall be a member of the Partnership and act as a liaison among the Partnership, the community, and the Federal Government.

(2) CHAIRPERSON AND VICE CHAIRPERSON.—The Partnership shall designate one member to serve as the chairperson and one member to serve as the vice chairperson of the Partnership.

(3) PARTICIPATION.—Members shall be appointed under paragraph (1)(A), and the Partnership shall develop procedures for conducting its activities, so as to ensure a balance among various sectors of the health care system so that no single sector unduly influences the recommendations of the Partnership.

(4) TERMS.—Members appointed under paragraph (1)(A) shall serve for 3 year terms, except that any member appointed to fill a vacancy for an unexpired term shall be appointed for the remainder of such term. A member may serve for not to exceed 180 days after the expiration of such member's term or until a successor has been appointed.

(5) OUTSIDE INVOLVEMENT.—The Partnership shall ensure an adequate opportunity for the partici-

pation of outside advisors, including individuals with expertise in—

(A) the protection of personal health information privacy;

(B) personal health information security;

(C) health care quality and patient safety, including individuals with expertise in utilizing health information technology to improve health care quality and patient safety;

(D) medical and clinical research data exchange; and

(E) developing health information technology standards and new health information technology.

(6) QUORUM.—Two-thirds of the members of the Partnership shall constitute a quorum for the purpose of conducting votes.

(c) STANDARDS AND IMPLEMENTATION SPECIFICATIONS.—

(1) SCHEDULE.—Not later than 90 days after the date of enactment of this title, the Partnership shall develop a schedule for the assessment of standards and implementation specifications under this section. The Partnership shall update such schedule annually. The Secretary shall publish such schedule

in the Federal Register and on the Internet website of the Department of Health and Human Services.

(2) FIRST YEAR RECOMMENDATIONS.—Consistent with the schedule published under paragraph (1) and not later than 1 year after date of enactment of this title, the Partnership shall recommend, and the Secretary shall review, such standards and implementation specifications.

(3) ONGOING RECOMMENDATIONS.—The Partnership shall review and modify, as appropriate but at least annually, adopted standards and implementation specifications and continue to recommend additional standards and implementation specifications, consistent with the schedule published pursuant to paragraph (1). The Secretary shall review such modifications and recommendations.

(4) RECOGNITION OF PRIVATE ENTITIES.—The Partnership, in consultation with the Secretary, may recognize a private entity or entities for the purpose of developing and updating standards and implementation specifications to achieve uniform and consistent implementation of the standards adopted by the President under this title. Such entity or entities shall make recommendations to the Partnership consistent with this section.

(5) PUBLICATION.—All recommendations made by the Partnership pursuant to this section shall be published in the Federal Register and on the Internet website of the Office of the National Coordinator.

(6) REQUIREMENT FOR CERTAIN RECOMMENDATIONS.—The Partnership may not issue any recommendation that affects an individual's right to health information privacy unless such recommendation receives the affirmative support of the consumer or patient organization representative of the Partnership appointed under subsection (b)(1)(A)(vi)(I).

(7) PILOT TESTING.—The Secretary may conduct, or recognize a private entity or entities to conduct, a pilot project to test the standards and implementation specifications developed under this section in order to provide for the efficient implementation of the standards and implementation specifications described in this subsection prior to issuing such recommendations.

(8) PUBLIC INPUT.—The Partnership shall conduct open public meetings and develop a process to allow for public comment on the schedule and recommendations described in this section. Such proc-

ess shall ensure that such comments will be submitted within 30 days of the publication of a recommendation under this section.

(9) FEDERAL ACTION.—Not later than 90 days after the issuance of a recommendation from the Partnership under this subsection, the Secretary, in collaboration with representatives of other relevant Federal agencies as determined appropriate by the President, shall jointly review such recommendation. If appropriate, the President shall provide for the adoption by the Federal Government of any standard or implementation specification contained in such recommendation only after providing an opportunity for public comment in accordance with section 553 of title 5, United States Code. Such determination shall be published in the Federal Register and on the Internet website of the Office of the National Coordinator within 30 days after such determination is made.

(10) CONSISTENCY.—The standards and implementation specifications described in this subsection shall be consistent with the privacy protections in title I and the standards for information transactions and data elements developed pursuant to the regulations promulgated under section 264(c) of the

Health Insurance Portability and Accountability Act of 1996.

(d) CERTIFICATION.—

(1) DEVELOPING CRITERIA.—The Partnership, in consultation with the Secretary, may recognize a private entity or entities for the purpose of developing and recommending to the Partnership criteria to certify that appropriate categories of health information technology products that claim to be in compliance with applicable standards and implementation specifications adopted under this title have established such compliance.

(2) ADOPTION OF CRITERIA.—The Secretary, based upon the recommendations of the Partnership, shall review, and if appropriate, adopt such criteria.

(3) CONDUCTING CERTIFICATION.—The Secretary may recognize a private entity or entities to conduct the certifications described under paragraph (1) using the criteria adopted by the Secretary under this subsection.

(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed as disrupting existing activities described in subsection (c) or (d).

(f) REQUIREMENT TO CONSIDER RECOMMENDATIONS.—In carrying out the activities described in sub-

sections (c) and (d), the Partnership shall adopt and integrate the recommendations of the American Health Information Community that are adopted by the Secretary.

(g) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section, $2,000,000 for each of the fiscal years 2009 and 2010.

SEC. 203. AMERICAN HEALTH INFORMATION COMMUNITY POLICIES.

(a) ESTABLISHMENT.—There is established a committee to be known as the American Health Information Community (in this section referred to as the ''Community''). The Community shall—

(1) provide advice to the Secretary and the heads of any relevant Federal agencies concerning the policy considerations related to health information technology;

(2) not later than 1 year after the date of enactment of this title, and annually thereafter, make recommendations concerning a policy framework for the development and adoption of a nationwide interoperable health information technology infrastructure;

(3) not later than 1 year after the date of enactment of this title, and annually thereafter, make recommendation concerning national policies for

adoption by the Federal Government, and voluntary adoption by private entities, to support the widespread adoption of health information technology, including—

(A) the protection of personal health information, including policies concerning the individual's ability to control the acquisition, uses, and disclosures of personal health information;

(B) methods to protect personal health information from improper use and disclosures and methods to notify patients if their personal health information is wrongfully disclosed;

(C) methods to facilitate and secure access to such individual's personal health information;

(D) the appropriate uses of a nationwide personal health information infrastructure including—

(i) the collection of quality data and public reporting;

(ii) biosurveillance and public health;

(iii) medical and clinical research; and

(iv) drug safety;

(E) fostering the public understanding of health information technology;

(F) strategies to enhance the use of health information technology in preventing and managing chronic disease;

(G) policies to incorporate the input of employees of health care providers in the design and implementation of health information technology systems; and

(H) other policies determined to be necessary by the Community; and

(4) serve as a forum for the participation of a broad range of stakeholders to provide input on improving the effective implementation of health information technology systems.

The Community may not make any recommendation that affects an individual's right to health information privacy unless the recommendation receives the affirmative support of the consumer or patient organization representative appointed under subsection (c)(1)(A)(viii)(I).

(b) PUBLICATION.—All recommendations made by the Community pursuant to this section shall be published in the Federal Register and on the Internet website of the National Coordinator. The Secretary shall review all recommendations and determine which recommendations shall be endorsed by the Federal Government and such determination shall be published on the Internet website

of the Office of the National Coordinator after an opportunity for public comment in accordance with section 553 of title 5, United States Code.

(c) MEMBERSHIP.—

(1) MEMBERS.—The members of the Community shall consist of the following:

(A) APPOINTED MEMBERS.—The appointed members of the Community shall be appointed as follows:

(i) 3 members shall be appointed by the Secretary, 1 of whom shall be a representative from the Department of Health and Human Services.

(ii) 1 member shall be appointed by the Secretary of Veterans Affairs who shall represent the Department of Veterans Affairs.

(iii) 1 member shall be appointed by the Secretary of Defense who shall represent the Department of Defense.

(iv) 1 member shall be appointed by the majority leader of the Senate.

(v) 1 member shall be appointed by the minority leader of the Senate.

(vi) 1 member shall be appointed by the Speaker of the House of Representatives.

(vii) 1 member shall be appointed by the minority leader of the House of Representatives.

(viii) Nine members shall be appointed by the Comptroller General of whom—

(I) one member shall be advocates for patients or consumers;

(II) one member shall represent health care providers;

(III) one member shall be from a labor organization representing health care workers;

(IV) one member shall have expertise in the protection of privacy and data security;

(V) one member shall have expertise in improving the health of vulnerable populations;

(VI) one member shall represent health plans or other third party payers;

(VII) one member shall represent information technology vendors;

(VIII) one member shall represent purchasers or employers; and

(IX) one member shall have expertise in health care quality measurement and reporting.

(B) NATIONAL COORDINATOR.—The National Coordinator shall be a member of the Community and act as a liaison among the Community, the partnership, and the Federal Government.

(2) CHAIRPERSON AND VICE CHAIRPERSON.—The Community shall designate one member to serve as the chairperson and one member to serve as the vice chairperson of the Community.

(3) PARTICIPATION.—The members of the Community appointed under paragraph (1) shall represent a balance among various sectors of the health care system so that no single sector unduly influences the recommendations of the Community.

(4) TERMS.—

(A) IN GENERAL.—The terms of members of the Community shall be for 3 years except that the Comptroller General shall designate

staggered terms for the members first appointed.

(B) VACANCIES.—Any member appointed to fill a vacancy in the membership of the Community that occurs prior to the expiration of the term for which the member's predecessor was appointed shall be appointed only for the remainder of that term. A member may serve after the expiration of that member's term until a successor has been appointed. A vacancy in the Community shall be filled in the manner in which the original appointment was made.

(5) OUTSIDE INVOLVEMENT.—The Community shall ensure an adequate opportunity for the participation of outside advisors, including individuals with expertise in—

(A) the protection of health information privacy and security;

(B) improving the health of vulnerable populations;

(C) health care quality and patient safety, including individuals with expertise in measurement and the use of health information technology to capture data to improve health care quality and patient safety;

(D) ethics, including the ethical standards of professional medical and mental health practitioner associations;

(E) medical and clinical research data exchange;

(F) developing health information technology standards and new health information technology; and

(G) the operation of a State or local health information network.

(6) QUORUM.—Ten members of the Community shall constitute a quorum for purposes of voting, but a lesser number of members may meet and hold hearings.

(d) FEDERAL AGENCIES.—

(1) STAFF OF OTHER FEDERAL AGENCIES.—Upon the request of the Community, the head of any Federal agency may detail, without reimbursement, any of the personnel of such agency to the Community to assist in carrying out the duties of the Community. Any such detail shall not interrupt or otherwise affect the civil service status or privileges of the Federal employee involved.

(2) TECHNICAL ASSISTANCE.—Upon the request of the Community, the head of a Federal

agency shall provide such technical assistance to the Community as the Community determines to be necessary to carry out its duties.

(3) OTHER RESOURCES.—The Community shall have reasonable access to materials, resources, statistical data, and other information from the Library of Congress and agencies and elected representatives of the executive and legislative branches of the Federal Government. The chairperson or vice chairperson of the Community shall make requests for such access in writing when necessary.

(e) APPLICATION OF FACA.—The Federal Advisory Committee Act (5 U.S.C. App.) shall apply to the Community, except that the term provided for under section 14(a)(2) of such Act shall be not longer than 7 years.

(f) SUNSET.—The provisions of this section shall not apply after September 20, 2014.

(g) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section, $2,000,000 for each of fiscal years 2009 and 2010.

SEC. 204. RESEARCH ACCESS TO HEALTH CARE DATA AND REPORTING ON PERFORMANCE.

The Secretary shall permit researchers that meet criteria used to evaluate the appropriateness of the release

data for research purpose (as established by the Secretary) to—

(1) have access to all Federal health care data; and

(2) report on the performance of health care providers and suppliers, including reporting in a provider- or supplier-identifiable format.

Subtitle B—Facilitating the Widespread Adoption of Interoperable Health Information Technology

SEC. 211. FACILITATING THE WIDESPREAD ADOPTION OF INTEROPERABLE HEALTH INFORMATION TECHNOLOGY.

(a) COMPETITIVE GRANTS FOR ADOPTION OF TECHNOLOGY.—

(1) IN GENERAL.—The Secretary may award competitive grants to eligible entities to facilitate the purchase and enhance the utilization of qualified health information technology systems (as defined in section 213) to improve the quality and efficiency of health care.

(2) ELIGIBILITY.—To be eligible to receive a grant under paragraph (1) an entity shall—

(A) submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require;

(B) submit to the Secretary a strategic plan for the implementation of data sharing and interoperability measures;

(C) adopt the standards adopted by the Federal Government under section 301;

(D) implement the measures adopted under section 221 and report to the Secretary on such measures;

(E) comply with the requirements of title I;

(F) take into account the input of employees and staff who are directly involved in patient care of such health care providers in the design, implementation, and use of qualified health information technology systems;

(G) demonstrate significant financial need;

(H) provide matching funds in accordance with paragraph (4); and

(I) be a—

(i) public or not for profit hospital;

(ii) federally qualified health center (as defined in section 1861(aa)(4) of the Social Security Act);

(iii) individual or group practice (or a consortium thereof); or

(iv) another health care provider not described in clause (i) or (ii);

that serves medically undeserved communities.

(3) USE OF FUNDS.—Amounts received under a grant under this subsection shall be used to—

(A) facilitate the purchase of qualified health information technology systems;

(B) train personnel in the use of such systems;

(C) enhance the utilization of qualified health information technology systems (which may include activities to increase the awareness among consumers of health care privacy protections); or

(D) improve the prevention and management of chronic disease.

(4) MATCHING REQUIREMENT.—To be eligible for a grant under this subsection an entity shall contribute non-Federal contributions to the costs of carrying out the activities for which the grant is award-

ed in an amount equal to $1 for each $3 of Federal funds provided under the grant.

(5) PREFERENCE IN AWARDING GRANTS.—In awarding grants under this subsection the Secretary shall give preference to—

(A) eligible entities that will improve the degree to which such entity will link the qualified health information technology system to local or regional health information plan or plans; and

(B) with respect to awards made for the purpose of providing care in an outpatient medical setting, entities that organize their practices as a patient-centered medical home.

(b) COMPETITIVE GRANTS FOR THE DEVELOPMENT OF STATE LOAN PROGRAMS TO FACILITATE THE WIDESPREAD ADOPTION OF HEALTH INFORMATION TECHNOLOGY.—

(1) IN GENERAL.—The Secretary may award competitive grants to States for the establishment of State programs for loans to health care providers to facilitate the purchase and enhance the utilization of qualified health information technology.

(2) ESTABLISHMENT OF FUND.—To be eligible to receive a competitive grant under this subsection,

a State shall establish a qualified health information technology loan fund (referred to in this subsection as a ''State loan fund'') and comply with the other requirements contained in this subsection. Amounts received under a grant under this subsection shall be deposited in the State loan fund established by the State. No funds authorized by other provisions of this title to be used for other purposes specified in this title shall be deposited in any such State loan fund.

(3) ELIGIBILITY.—To be eligible to receive a grant under paragraph (1) a State shall—

(A) submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require;

(B) submit to the Secretary a strategic plan in accordance with paragraph (4);

(C) establish a qualified health information technology loan fund in accordance with paragraph (2);

(D) require that health care providers receiving loans under the grant—

(i) link, to the extent practicable, the qualified health information system to a

local or regional health information network;

(ii) consult, as needed, with the Health Information Technology Resource Center established in section 914(d) to access the knowledge and experience of existing initiatives regarding the successful implementation and effective use of health information technology;

(iii) agree to notify individuals if their personal health information is wrongfully disclosed; and

(iv) take into account the input of employees and staff who are directly involved in patient care of such health care providers in the design and implementation and use of qualified health information technology systems;

(E) require that health care providers receiving loans under the grant adopt the standards adopted by the Federal Government under section 301;

(F) require that health care providers receiving loans under the grant implement the

measures adopted under section 221 and report to the Secretary on such measures; and

(G) provide matching funds in accordance with paragraph (8).

(4) STRATEGIC PLAN.—

(A) IN GENERAL.—A State that receives a grant under this subsection shall annually prepare a strategic plan that identifies the intended uses of amounts available to the State loan fund of the State.

(B) CONTENTS.—A strategic plan under subparagraph (A) shall include—

(i) a list of the projects to be assisted through the State loan fund in the first fiscal year that begins after the date on which the plan is submitted;

(ii) a description of the criteria and methods established for the distribution of funds from the State loan fund;

(iii) a description of the financial status of the State loan fund and the short-term and long-term goals of the State loan fund; and

(iv) a description of the strategies the State will use to address challenges in the

adoption of health information technology due to limited broadband access.

(5) USE OF FUNDS.—

(A) IN GENERAL.—Amounts deposited in a State loan fund, including loan repayments and interest earned on such amounts, shall be used only for awarding loans or loan guarantees, or as a source of reserve and security for leveraged loans, the proceeds of which are deposited in the State loan fund established under paragraph (1). Loans under this section may be used by a health care provider to—

(i) facilitate the purchase of qualified health information technology systems;

(ii) enhance the utilization of qualified health information technology systems (which may include activities to increase the awareness among consumers of health care of privacy protections and privacy rights); or

(iii) train personnel in the use of such systems.

(B) LIMITATION.—Amounts received by a State under this subsection may not be used—

(i) for the purchase or other acquisition of any health information technology system that is not a qualified health information technology system;

(ii) to conduct activities for which Federal funds are expended under this title, or the amendments made by this title; or

(iii) for any purpose other than making loans to eligible entities under this section.

(6) TYPES OF ASSISTANCE.—Except as otherwise limited by applicable State law, amounts deposited into a State loan fund under this subsection may only be used for the following:

(A) To award loans that comply with the following:

(i) The interest rate for each loan shall be less than or equal to the market interest rate.

(ii) The principal and interest payments on each loan shall commence not later than 1 year after the date on which the loan was awarded, and each loan shall

be fully amortized not later than 10 years after such date.

(iii) The State loan fund shall be credited with all payments of principal and interest on each loan awarded from the fund.

(B) To guarantee, or purchase insurance for, a local obligation (all of the proceeds of which finance a project eligible for assistance under this subsection) if the guarantee or purchase would improve credit market access or reduce the interest rate applicable to the obligation involved.

(C) As a source of revenue or security for the payment of principal and interest on revenue or general obligation bonds issued by the State if the proceeds of the sale of the bonds will be deposited into the State loan fund.

(D) To earn interest on the amounts deposited into the State loan fund.

(7) ADMINISTRATION OF STATE LOAN FUNDS.—

(A) COMBINED FINANCIAL ADMINISTRATION.—A State may (as a convenience and to avoid unnecessary administrative costs) com-

bine, in accordance with State law, the financial administration of a State loan fund established under this subsection with the financial administration of any other revolving fund established by the State if not otherwise prohibited by the law under which the State loan fund was established.

(B) COST OF ADMINISTERING FUND.—Each State may annually use not to exceed 4 percent of the funds provided to the State under a grant under this subsection to pay the reasonable costs of the administration of the programs under this section, including the recovery of reasonable costs expended to establish a State loan fund which are incurred after the date of enactment of this title.

(C) GUIDANCE AND REGULATIONS.—The Secretary shall publish guidance and promulgate regulations as may be necessary to carry out the provisions of this subsection, including—

(i) provisions to ensure that each State commits and expends funds allotted to the State under this subsection as effi-

ciently as possible in accordance with this title and applicable State laws; and

(ii) guidance to prevent waste, fraud, and abuse.

(D) PRIVATE SECTOR CONTRIBUTIONS.—

(i) IN GENERAL.—A State loan fund established under this subsection may accept contributions from private sector entities, except that such entities may not specify the recipient or recipients of any loan issued under this subsection.

(ii) AVAILABILITY OF INFORMATION.—A State shall make publicly available the identity of, and amount contributed by, any private sector entity under clause (i) and may issue letters of commendation or make other awards (that have no financial value) to any such entity.

(8) MATCHING REQUIREMENTS.—

(A) IN GENERAL.—The Secretary may not make a grant under paragraph (1) to a State unless the State agrees to make available (directly or through donations from public or private entities) non-Federal contributions in cash toward the costs of the State program to be im-

plemented under the grant in an amount equal to not less than $1 for each $1 of Federal funds provided under the grant.

(B) DETERMINATION OF AMOUNT OF NON-FEDERAL CONTRIBUTION.—In determining the amount of non-Federal contributions that a State has provided pursuant to subparagraph (A), the Secretary may not include any amounts provided to the State by the Federal Government.

(9) PREFERENCE IN AWARDING GRANTS.—The Secretary may give a preference in awarding grants under this subsection to States that adopt value-based purchasing programs to improve health care quality.

(10) REPORTS.—The Secretary shall annually submit to the Committee on Health, Education, Labor, and Pensions and the Committee on Finance of the Senate, and the Committee on Energy and Commerce and the Committee on Ways and Means of the House of Representatives, a report summarizing the reports received by the Secretary from each State that receives a grant under this subsection.

(c) COMPETITIVE GRANTS FOR THE IMPLEMENTATION OF REGIONAL OR LOCAL HEALTH INFORMATION TECHNOLOGY PLANS.—

(1) IN GENERAL.—The Secretary may award competitive grants to eligible entities to implement regional or local health information plans to improve health care quality and efficiency through the electronic exchange of personal health information pursuant to the standards, implementation specifications and certification criteria, and other requirements adopted by the Secretary under section 221.

(2) ELIGIBILITY.—To be eligible to receive a grant under paragraph (1) an entity, which may be a health record bank or trust, shall—

(A) demonstrate financial need to the Secretary;

(B) demonstrate that one of its principal missions or purposes is to use information technology to improve health care quality and efficiency;

(C) adopt bylaws, memoranda of understanding, or other charter documents that demonstrate that the governance structure and decision making processes of such entity allow for

participation on an ongoing basis by multiple stakeholders within a community, including—

(i) health care providers (including health care providers that provide services to low income and undeserved populations);

(ii) pharmacists or pharmacies;

(iii) health plans;

(iv) health centers (as defined in section 330(b)) and federally qualified health centers (as defined in section 1861(aa)(4) of the Social Security Act) and rural health clinics (as defined in section 1861(aa) of the Social Security Act), if such centers or clinics are present in the community served by the entity;

(v) patient or consumer organizations;

(vi) organizations dedicated to improving the health of vulnerable populations;

(vii) employers;

(viii) State or local health departments; and

(ix) any other health care providers or other entities, as determined appropriate by the Secretary;

(D) demonstrate the participation, to the extent practicable, of stakeholders in the electronic exchange of personal health information within the local or regional plan pursuant to subparagraph (C);

(E) adopt nondiscrimination and conflict of interest policies that demonstrate a commitment to open, fair, and nondiscriminatory participation in the health information plan by all stakeholders;

(F) adopt the standards adopted by the Secretary under section 301;

(G) require that health care providers receiving such grants—

(i) implement the measures adopted under section 221 and report to the Secretary on such measures; and

(ii) take into account the input of employees and staff who are directly involved in patient care of such health care providers in the design, implementation, and

use of health information technology systems;

(H) agree to comply with the requirements of title I;

(I) facilitate the electronic exchange of personal health information within the local or regional area and among local and regional areas;

(J) prepare and submit to the Secretary an application in accordance with paragraph (3);

(K) agree to provide matching funds in accordance with paragraph (5); and

(L) reduce barriers to the implementation of health information technology by providers.

(3) APPLICATION.—

(A) IN GENERAL.—To be eligible to receive a grant under paragraph (1), an entity shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

(B) REQUIRED INFORMATION.—At a minimum, an application submitted under this paragraph shall include—

(i) clearly identified short-term and long-term objectives of the regional or local health information plan;

(ii) a technology plan that complies with the standards, implementation specifications, and certification criteria adopted under section 202(c)(6) and that includes a descriptive and reasoned estimate of costs of the hardware, software, training, and consulting services necessary to implement the regional or local health information plan;

(iii) a strategy that includes initiatives to improve health care quality and efficiency, including the use and reporting of health care quality measures adopted under section 221;

(iv) a plan that describes provisions to encourage the implementation of the electronic exchange of personal health information by all health care providers participating in the health information plan;

(v) a plan to ensure the privacy and security of personal health information that is consistent with the requirements of title I;

(vi) a governance plan that defines the manner in which the stakeholders shall

jointly make policy and operational decisions on an ongoing basis;

(vii) a financial or business plan that describes—

(I) the sustain ability of the plan;

(II) the financial costs and benefits of the plan; and

(III) the entities to which such costs and benefits will accrue;

(viii) a description of whether the State in which the entity resides has received a grant under section 319D of the Public Health Service Act, alone or as a part of a consortium, and if the State has received such a grant, how the entity will coordinate the activities funded under such section 319D with the system under this section; and

(ix) in the case of an applicant entity that is unable to demonstrate the participation of all stakeholders pursuant to paragraph (2)(C), the justification from the entity for any such nonparticipation.

(4) USE OF FUNDS.—Amounts received under a grant under paragraph (1) shall be used to establish

and implement a regional or local health information plan in accordance with this subsection.

(5) MATCHING REQUIREMENT.—

(A) IN GENERAL.—The Secretary may not make a grant under this subsection to an entity unless the entity agrees that, with respect to the costs to be incurred by the entity in carrying out the network program for which the grant was awarded, the entity will make available (directly or through donations from public or private entities) non-Federal contributions toward such costs in an amount equal to not less than 50 percent of such costs ($1 for each $2 of Federal funds provided under the grant).

(B) DETERMINATION OF AMOUNT CONTRIBUTED.—Non-Federal contributions required under subparagraph (A) may be in cash or in kind, fairly evaluated, including equipment, technology, or services. Amounts provided by the Federal Government, or services assisted or subsidized to any significant extent by the Federal Government, may not be included in determining the amount of such non-Federal contributions.

(6) HEALTH RECORD BANK OR TRUST DEFINED.—In this section, the term ''health record bank or trust'' means an independent organization that provides a secure electronic repository for storing and maintaining an individual's lifetime health and medical records from multiple sources and ensuring that the individual always has complete control over who accesses their information.

(d) REPORTS.—Not later than 1 year after the date on which the first grant is awarded under this section, and annually thereafter during the grant period, an entity that receives a grant under this section shall submit to the Secretary a report on the activities carried out under the grant involved. Each such report shall include—

(1) a description of the financial costs and benefits of the project involved and of the entities to which such costs and benefits accrue;

(2) an analysis of the impact of the project on health care quality and safety;

(3) a description of any reduction in duplicative or unnecessary care as a result of the project involved; and

(4) other information as required by the Secretary.

(e) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—For the purpose of carrying out this section, there is authorized to be appropriated $139,000,000 for fiscal year 2009 and $139,000,000 for fiscal year 2010.

(2) AVAILABILITY.—Amounts appropriated under paragraph (1) shall remain available through fiscal year 2012.

SEC. 212. DEMONSTRATION PROGRAM TO INTEGRATE INFORMATION TECHNOLOGY INTO CLINICAL EDUCATION.

(a) IN GENERAL.—The Secretary may award grants to eligible entities or consortia under this section to carry out demonstration projects to develop academic curricula integrating qualified health information technology systems in the clinical education of health professionals or analyze clinical data sets to discover quality measures. Such awards shall be made on a competitive basis and pursuant to peer review.

(b) ELIGIBILITY.—To be eligible to receive a grant under subsection (a), an entity or consortium shall—

(1) submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require;

(2) be or include—

(A) a health professions school;

(B) a school of nursing; or

(C) an institution with a graduate medical education program;

(3) provide for the collection of data regarding the effectiveness of the demonstration project to be funded under the grant in improving the safety of patients and the efficiency of health care delivery; and

(4) provide matching funds in accordance with subsection (d).

(c) USE OF FUNDS.—

(1) IN GENERAL.—With respect to a grant under subsection (a), an eligible entity or consortium shall use amounts received under the grant in collaboration with 2 or more disciplines.

(2) LIMITATION.—An eligible entity or consortium shall not award a grant under subsection (a) to purchase hardware, software, or services.

(d) MATCHING FUNDS.—

(1) IN GENERAL.—The Secretary may award a grant to an entity under or consortium this section only if the entity of consortium agrees to make available non-Federal contributions toward the costs of the program to be funded under the grant in an

amount that is not less than $1 for each $2 of Federal funds provided under the grant.

(2) DETERMINATION OF AMOUNT CONTRIBUTED.—Non-Federal contributions under paragraph (1) may be in cash or in kind, fairly evaluated, including equipment or services. Amounts provided by the Federal Government, or services assisted or subsidized to any significant extent by the Federal Government, may not be included in determining the amount of such contributions.

(e) EVALUATION.—The Secretary shall take such action as may be necessary to evaluate the projects funded under this section and publish, make available, and disseminate the results of such evaluations on as wide a basis as is practicable.

(f) REPORTS.—Not later than 1 year after the date of enactment of this title, and annually thereafter, the Secretary shall submit to the Committee on Health, Education, Labor, and Pensions and the Committee on Finance of the Senate, and the Committee on Energy and Commerce and the Committee on Ways and Means of the House of Representatives a report that—

(1) describes the specific projects established under this section; and

(2) contains recommendations for Congress based on the evaluation conducted under subsection (e).

(g) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section, $2,000,000 for each of fiscal years 2009 and 2010.

(h) SUNSET.—This provisions of this section shall not apply after September 30, 2012.

SEC. 213. QUALIFIED HEALTH INFORMATION TECHNOLOGY SYSTEM DEFINED.

In this subtitle, the term ''qualified health information technology system'' means a computerized system (including hardware and software) that—

(1) safeguards the privacy, security, and confidentiality of personal health information in accordance with the requirements of title I;

(2) maintains and provides permitted access to health information in an electronic format;

(3) with respect to personal health information maintained in a designated record set, preserves an audit trail of each individual that has gained access to such record set;

(4) incorporates decision support to reduce medical errors and enhance health care quality;

(5) complies with the standards adopted by the Federal Government under section 202;

(6) has the ability to transmit and exchange information to other health information technology systems and, to the extent feasible, public health information technology systems; and

(7) allows for the reporting of quality measures adopted under section 221.

Subtitle C—Improving the Quality of Health Care

SEC. 221. FOSTERING DEVELOPMENT AND USE OF HEALTH CARE QUALITY MEASURES.

(a) IN GENERAL.—The Secretary shall provide for the development and use of health care quality measures (referred to in this title as ''quality measures'') for the purpose of measuring the quality and efficiency of health care that patients receive.

(b) DESIGNATION OF, AND ARRANGEMENT WITH, ORGANIZATION.—

(1) IN GENERAL.—Not later than 90 days after the date of enactment of this title, the Secretary shall designate, and have in effect an arrangement with, a single organization that meets the requirements of subsection (c) under which such organization shall promote the development of quality meas-

ures and provide the Secretary with advice and recommendations on the key elements and priorities of a national system for healthcare performance measurement.

(2) RESPONSIBILITIES.—The responsibilities to be performed by the organization designated under paragraph (1) (in this title referred to as the ''designated organization'') shall include—

(A) establishing and managing an integrated national strategy and process for setting priorities and goals in establishing quality measures;

(B) coordinating and harmonizing the development and testing of such measures;

(C) establishing standards for the development and testing of such measures;

(D) endorsing national consensus quality measures;

(E) recommending, in collaboration with multi-stakeholder groups, quality measures to the Secretary for adoption and use;

(F) promoting the development and use of electronic health records that contain the functionality for automated collection, aggrega-

tion, and transmission of performance measurement information; and

(G) providing recommendations and advice to the Partnership for Health Care Improvement regarding the integration of quality measures into the certification process outlined under section 202 and the American Health Information Community regarding national policies outlined under section 203.

(c) REQUIREMENTS DESCRIBED.—The requirements described in this subsection are the following:

(1) PRIVATE ENTITY.—The organization shall be a private nonprofit entity that is governed by a board of directors and an individual who is designated as president and chief executive officer.

(2) BOARD MEMBERSHIP.—The members of the board of directors of the entity shall include representatives of—

(A) health care providers or groups representing providers;

(B) health plans or groups representing health plans;

(C) patients or consumers enrolled in such plans or groups representing individuals enrolled in such plans;

(D) health care purchasers and employers or groups representing purchasers or employers; and

(E) organizations that develop health information technology standards and new health information technology.

(3) OTHER MEMBERSHIP REQUIREMENTS.—The membership of the board of directors of the entity shall be representative of individuals with experience with—

(A) urban health care issues;

(B) safety net health care issues;

(C) rural or frontier health care issues;

(D) quality and safety issues;

(E) State or local health programs;

(F) individuals or entities skilled in the conduct and interpretation of biomedical, health services, and health economics research and with expertise in outcomes and effectiveness research and technology assessment;

(G) individuals or entities involved in the development and establishment of standards and certification for health information technology systems and clinical data; and

(H) members of the medical and mental health professions with expertise in standards of professional ethics.

(4) OPEN AND TRANSPARENT.—With respect to matters related to the arrangement with the Secretary under subsection (a)(1), the organization shall conduct its business in an open and transparent manner, and provide the opportunity for public comment and ensure a balance among disparate stakeholders, so that no member organization unduly influences the work of the organization.

(5) VOLUNTARY CONSENSUS STANDARDS SETTING ORGANIZATIONS.—The organization shall operate as a voluntary consensus standards setting organization as defined for purposes of section 12(d) of the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113) and Office of Management and Budget Revised Circular A-119 (published in the Federal Register on February 10, 1998).

(6) PARTICIPATION.—If the organization requires a fee for membership, the organization shall ensure that such fee is not a substantial barrier to participation in the entity's activities related to the arrangement with the Secretary.

(d) REQUIREMENTS FOR MEASURES.—The quality measures developed under this title shall comply with the following:

(1) MEASURES.—The designated organization, in promoting the development of quality measures under this title, shall ensure that such measures—

(A) are evidence-based, reliable, and valid;

(B) include—

(i) measures of clinical processes and outcomes, patient experience, efficiency, and equity; and

(ii) measures to assess effectiveness, timeliness, patient self-management, patient centeredness, and safety; and

(C) include measures of underuse and overuse.

(2) PRIORITIES.—In carrying out its responsibilities under this section, the designated organization shall ensure that priority is given to—

(A) measures that preserve access to quality health care by protecting the privacy and security of personal health information;

(B) measures with the greatest potential impact for improving the performance and efficiency of care;

(C) measures that may be rapidly implemented by group health plans, health insurance issuers, physicians, hospitals, nursing homes, long-term care providers, and other providers;

(D) measures which may inform health care decisions made by consumers and patients;

(E) measures that apply to multiple services furnished by different providers during an episode of care;

(F) measures that can be integrated into certification process described in section 202; and

(G) measures that may be integrated into the decision support function of qualified health information technology as defined by this title.

(3) RISK ADJUSTMENT.—The designated organization, in consultation with performance measure developers and other stakeholders, shall establish procedures to ensure that quality measures take into account differences in patient health status, patient characteristics, and geographic location, as appropriate.

(4) MAINTENANCE.—The designated organization, in consultation with owners and developers of quality measures, shall require the owners or devel-

opers of quality measures to update and enhance such measures, including the development of more accurate and precise specifications, and retire existing outdated measures. Such updating shall occur not more often than once during each 12-month period, except in the case of emergency circumstances requiring a more immediate update to a measure.

(e) GRANTS FOR PERFORMANCE MEASURE DEVELOPMENT.—The Secretary, acting through the Agency for Healthcare Research and Quality, may award grants, in amounts not to exceed $50,000 each, to organizations to support the development and testing of quality measures that meet the standards established by the designated organization.

SEC. 222. ADOPTION AND USE OF QUALITY MEASURES; REPORTING.

(a) IN GENERAL.—For purposes of carrying out activities authorized or required by this title to ensure the use of quality measures and to foster uniformity between health care quality measures utilized by private entities, the Secretary shall—

(1) select quality measures for adoption and use, from quality measures recommended by multi-stakeholder groups and endorsed by the designated organization; and

(2) ensure that standards adopted under section 301 integrate the quality measures endorsed, adopted, and utilized under this section.

(b) RELATIONSHIP WITH PROGRAMS UNDER THE SOCIAL SECURITY ACT.—The Secretary shall ensure that the quality measures adopted under this section—

(1) complement quality measures developed by the Secretary under programs administered by the Secretary under the Social Security Act, including programs under titles XVIII, XIX, and XXI of such Act; and

(2) do not conflict with the needs and priorities of the programs under titles XVIII, XIX, and XXI of such Act, as set forth by the Administrator of the Centers for Medicare & Medicaid Services.

(c) REPORTING.—The Secretary shall implement procedures, consistent with generally accepted standards, to enable the Department of Health and Human Services to accept the electronic submission of data for purposes of performance measurement, including at the provider level, using the quality measures developed, endorsed, and adopted pursuant to this title.

(d) DISSEMINATION OF INFORMATION.—In order to make comparative performance information available to health care consumers, health professionals, public health

officials, oversight organizations, researchers, and other appropriate individuals and entities, after consultation with multi-stakeholder groups, the Secretary shall promulgate regulations to provide for the dissemination, aggregation, and analysis of quality measures collected pursuant to this title.

Subtitle D—Miscellaneous Provisions

SEC. 231. HEALTH INFORMATION TECHNOLOGY RESOURCE CENTER.

Section 914 of the Public Health Service Act (42 U.S.C. 299b-3) is amended by adding at the end the following:

''(d) HEALTH INFORMATION TECHNOLOGY RESOURCE CENTER.—

''(1) IN GENERAL.—The Secretary, acting through the Director, shall develop a Health Information Technology Resource Center (referred to in this subsection as the 'Center') to provide technical assistance and develop best practices to support and accelerate efforts to adopt, implement, and effectively use interoperable health information technology in compliance with sections 202 and 221 of the TRUST in Health Information Act of 2008.

''(2) PURPOSES.—The purposes of the Center are to—

''(A) provide a forum for the exchange of knowledge and experience;

''(B) accelerate the transfer of lessons learned from existing public and private sector initiatives, including those currently receiving Federal financial support;

''(C) assemble, analyze, and widely disseminate evidence and experience related to the adoption, implementation, and effective use of interoperable health information technology;

''(D) provide for the establishment of regional and local health information networks to facilitate the development of interoperability across health care settings and improve the quality of health care;

''(E) provide for the development of solutions to barriers to the exchange of electronic health information; and

''(F) conduct other activities identified by the States, local, or regional health information networks, or health care stakeholders as a focus for developing and sharing best practices.

''(3) SUPPORT FOR ACTIVITIES.—To provide support for the activities of the Center, the Director shall modify the requirements, if necessary, that apply to the National Resource Center for Health Information Technology to provide the necessary infrastructure to support the duties and activities of the Center and facilitate information exchange across the public and private sectors.

''(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to require the duplication of Federal efforts with respect to the establishment of the Center, regardless of whether such efforts were carried out prior to or after the enactment of this subsection.

''(e) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated, such sums as may be necessary for each of fiscal years 2009 and 2010 to carry out this section.''.

SEC. 232. FACILITATING THE PROVISION OF TELEHEALTH SERVICES ACROSS STATE LINES.

Section 330L of the Public Health Service Act (42 U.S.C. 254c-18) is amended to read as follows:

"SEC. 330L. TELEMEDICINE; INCENTIVE GRANTS REGARDING COORDINATION AMONG STATES.

''(a) FACILITATING THE PROVISION OF TELEHEALTH SERVICES ACROSS STATE LINES.—The Secretary may make grants to States that have adopted regional State reciprocity agreements for practitioner licensure, in order to expedite the provision of telehealth services across State lines.

''(b) AUTHORIZATION OF APPROPRIATIONS.—For the purpose of carrying out subsection (a), there are authorized to be appropriated such sums as may be necessary for each of the fiscal years 2009 and 2010.''.

Subtitle E—Definitions

SEC. 241. DEFINITIONS.

In this title, the following terms, defined in section 171, have the meanings given such terms in such section: Breach , confidentiality, de-identified health information, disclose, Director of the Office of Health Information Privacy, employer, health care, health care provider, Office of Health Information Privacy, privacy, personal health information, Secretary, security, State, and use.

TITLE III—ADDITIONAL PROVISIONS

SEC. 301. FEDERAL PURCHASING AND DATA COLLECTION BY CMS AND OTHER FEDERAL AGENCIES.

(a) COORDINATION OF FEDERAL SPENDING.—

(1) IN GENERAL.—Not later than 1 year after the adoption by the President of a recommendation under section 202(c)(6), the Administrator of the Center for Medicare & Medicaid Services and the head of any other Federal agency shall not expend Federal funds for the purchase of any new health information technology or health information technology system for clinical care or for the electronic retrieval, storage, or exchange of personal health information if such technology or system is not consistent with applicable standards adopted by the Federal Government under section 202.

(2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to restrict the purchase of minor (as determined by the Secretary) hardware or software components in order to modify, correct a deficiency in, or extend the life of existing hardware or software.

(b) VOLUNTARY ADOPTION.—

(1) IN GENERAL.—Any standards and implementation specifications adopted by the Federal Government under section 202(c) shall be voluntary with respect to private entities.

(2) REQUIREMENT.—Private entities that enter into a contract with the Federal Government shall

adopt the standards and implementation specifications adopted by the Federal Government under this section for the purpose of activities under such Federal contract.

(3) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to require that a private entity that enters into a contract with the Federal Government adopt the standards and implementation specifications adopted by the Federal Government under this section with respect to activities not related to the contract.

(c) COORDINATION OF FEDERAL DATA COLLECTION.—Not later than 3 years after the adoption by the Federal Government of a recommendation as provided for in section 202(c), all Federal agencies (including the Center for Medicare & Medicaid Services) collecting health data in an electronic format for the purposes of quality reporting, surveillance, epidemiology, adverse event reporting, research, or for other purposes determined appropriate by the Secretary, shall comply with the standards and implementation specifications adopted under such subsection.

SEC. 302. ENSURING HEALTH CARE PROVIDERS PARTICIPATING IN THE MEDICARE PROGRAM MAY MAINTAIN HEALTH INFORMATION IN ELECTRONIC FORM.

Section 1871 of the Social Security Act (42 U.S.C. 1395hh) is amended by adding at the end the following new subsection:

''(g)(1) Any provider of services or supplier shall be deemed as meeting any requirement for the maintenance of data in paper form under this title (whether or not for purposes of management, billing, reporting, reimbursement, or otherwise) if the required data is maintained in an electronic form.

''(2) Nothing in this subsection shall be construed as requiring health care providers to maintain or submit data in electronic form.''.