To provide individuals with access to health information of which they are a subject, ensure personal privacy with respect to health related information, promote the use of non-identifiable information for health research, impose criminal and civil penalties for unauthorized use of protected health information, to provide for the strong enforcement of these rights, and to protect States' rights.

IN THE SENATE OF THE UNITED STATES

JULY 18 (legislative day, JULY 17), 2007

Mr. LEAHY (for himself and Mr. KENNEDY) introduced the following bill; which was read twice and referred to the Committee on Health, Education, Labor, and Pensions

A BILL

To provide individuals with access to health information of which they are a subject, ensure personal privacy with respect to health related information, promote the use of non-identifiable information for health research, impose criminal and civil penalties for unauthorized use of protected health information, to provide for the strong enforcement of these rights, and to protect States’ rights.

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 “Health Information Privacy and Security Act”.

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

Sec. 1. Short title.
Sec. 2. Purposes.
Sec. 3. Definitions.

TITLE I—INDIVIDUALS’ RIGHTS

Subtitle A—Rights of the Subjects of Protected Health Information

Sec. 101. Right to privacy and security.
Sec. 102. Inspection and copying of protected health information.
Sec. 103. Modifications to protected health information.
Sec. 104. Notice of privacy practices.
Sec. 105. Demonstration grant.

Subtitle B—Establishment of Safeguards

Sec. 111. Establishment of safeguards.
Sec. 112. Transparency.
Sec. 113. Risk management.
Sec. 114. Accounting for disclosures and use.

TITLE II—RESTRICTIONS ON USE AND DISCLOSURE

Subtitle A—General Restrictions on Use and Disclosure

Sec. 201. General rules regarding use and disclosure.
Sec. 203. Authorizations for disclosure of protected health information other than for treatment or payment.
Sec. 204. Notification in the case of breach.

Subtitle B—Disclosure Under Special Circumstances

Sec. 211. Emergency circumstances.
Sec. 212. Public health.
Sec. 213. Protection and advocacy agencies.
Sec. 214. Oversight.
Sec. 215. Disclosure for law enforcement, national security, and intelligence purposes.
Sec. 216. Next of kin and directory information.
Sec. 217. Health research.
Sec. 218. Judicial and administrative purposes.
Sec. 219. Individual representatives.

TITLE III—OFFICE OF HEALTH INFORMATION PRIVACY OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
SEC. 2. PURPOSES.

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 rights must be protected.

(2) To create incentives to turn protected health information into de-identified health information, where appropriate.

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

(4) To provide individuals with—

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

(5) To provide individuals with the right to limit the use and disclosure of protected health information.

(6) To establish strong and effective mechanisms to protect against the unauthorized and inappropriate use of protected health information.

(7) 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 address violations of the rights of individuals to privacy, to provide individuals with access to their health information, and to prevent the unauthorized use of protected health information that is genetic information.

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

(9) To protect the rights of States.

SEC. 3. DEFINITIONS.

In this Act:
(1) Administrative billing information.—

The term “administrative billing information” means any of the following forms of protected health information:

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

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

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

(D) Total billed charges.

(2) 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, the term includes the employees of the employer.

(3) Authorization.—The term “authorization” means the authority granted by an individual that is the subject of protected health information, in accordance with title II, for the disclosure of the individual’s protected health information.
(4) Authorized recipient.—The term “authorized recipient” means a person granted the authority by an individual, in accordance with title II, to access, maintain, retain, modify, record, store, destroy, or otherwise use the individual’s protected health information through an authorized disclosure.

(5) Breach.—The term “breach” means the unauthorized acquisition, disclosure, or loss of protected health information which compromises the security, privacy, or integrity of protected health information maintained by or on behalf of a person.

(6) Confidentiality.—The term “confidentiality” means the obligations of those who receive information to respect the privacy interests of those to whom the data relate.

(7) Data broker.—The term “data broker” 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 protected health information of individuals. Any person maintaining protected 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 prod-
ucts and services, shall be deemed to be a data
broker subject to the requirements of this Act.

(8) DE-IDENTIFIED HEALTH INFORMATION.—

(A) IN GENERAL.—The term “de-identified
health information” means any protected health
information, with respect to which—

(i) all personal identifiers, or other in-
formation that may be used by itself or in
combination with other information which
may be available to re-identify the subject
of the information, have been removed;

(ii) 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 accept-
ed scientific and statistical standards and
methods for minimizing risk of disclosure;
and

(iii) there is no reasonable basis to be-
lieve that the information can be used to
identify an individual.
(B) EXAMPLES.—Such term includes aggregate statistics, redacted health information, information in which random or fictitious alternatives have been substituted for personally identifiable information, and information in which personally identifiable information has been encrypted and the decryption key is maintained only by persons otherwise authorized to have access to such protected health information in an identifiable format.

(9) 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 protected 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 redisclosure of protected health information.

(10) DECRYPTION KEY.—The term “deryption key” means the variable information used in or produced by a mathematical formula, code, or algorithm, or any component thereof, used for encryption or decryption of wire, electronic, or other communications or stored information.
(11) **EMPLOYER.**—The term “employer” means a person that is engaged in business affecting commerce and that has employees.

(12) **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.

(13) **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.

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

(14) HEALTH CARE PROVIDER.—The term
“health care provider” means a person that, with re-
spect to a specific item of protected health informa-
tion, receives, accesses, maintains, retains, modifies,
records, stores, destroys, or otherwise uses or dis-
closes 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) contractors and other health care pro-
viders or facilities authorized to provide items
or services related to diagnosis or treatment of
a health concern, including hospitals, nursing
facilities, allied health professionals, and facili-
ties 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 health information; or

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

(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, or related activities and items; 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 plan.**—The term “health plan” has the meaning given such term for purposes of the regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996.

(18) **Health record set.**—The term “health record set” means any item, collection, or grouping of information that includes protected health information, such as an electronic health record, electronic medical record, personal health record, or ac-
count 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, school or university, data broker, or other person.

(19) Health researcher.—The term “health researcher” means a person that, with respect to a specific item of protected health information, receives the information—

(A) pursuant to section 217 (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.

(20) Informed consent.—The term “informed consent” means the authorization for use or disclosure of protected health information by the individual who is the subject of such information, conditioned upon that individual’s having been informed of the nature and probability of harm to the individual resulting from such authorization.

(21) Law enforcement inquiry.—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.

(22) Office of Health Information Privacy.—The term “Office of Health Information Pri-

vacy” means the Office of Health Information Pri-

vacy designated under section 301.

(23) Person.—The term “person” means an

entity that is a government, governmental subdivi-
sion of an executive branch agency or authority, cor-

poration, company, association, firm, partnership,
society, estate, trust, joint venture, individual, indi-

vidual representative, tribal government, and any

other legal entity. Such term also includes the em-

ployees, contractors, agents, and affiliates of all legal

entities described in the preceding sentence, whether

or not they are acting in the capacity of their em-

ployment, contract, agency, or affiliation.

(24) Privacy.—The term “privacy” means an

individual’s right to control the acquisition, uses, or
disclosures of his or her identifiable health data.

(25) Protected Health Information.—

(A) In General.—The term “protected

health information” means any information, in-
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, school or university, health care clearinghouse, health oversight agency, public health authority, employer, data broker, or other person or such person’s agent, officer, or employee; 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) DECRYPTION KEY.—The term “protected health information” includes any information described in paragraph (8).

(26) 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.

(27) 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).
(28) School or University.—The term “school or university” means an institution or place for instruction or education, including an elementary school, secondary school, or institution of higher education, a college, or an assemblage of colleges united under one corporate organization or government.

(29) Secretary.—The term “Secretary” means the Secretary of Health and Human Services.

(30) Security.—The term “security” means physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure.

(31) Security breach.—The term “security breach” means the physical, structural, or substantive compromise of the security of protected 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 protected health information by an unauthorized person, so long as no further use or disclosure is made by such person.
(32) **STATE.**—The term “State” includes 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 protected health information.

(35) **WRITING.**—The term “writing” means writing in either a paper-based or computer-based form, including electronic and digital signatures.

**TITLE I—INDIVIDUALS’ RIGHTS**

**Subtitle A—Rights of the Subjects of Protected Health Information**

**SEC. 101. RIGHT TO PRIVACY AND SECURITY.**

(a) **IN GENERAL.**—Individuals who are the subject of protected health information have the right to—
(1) privacy and security with respect to the use and disclosure of such information;

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

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

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

SEC. 102. INSPECTION AND COPYING OF PROTECTED HEALTH INFORMATION.

(a) RIGHT OF INDIVIDUAL.—

(1) IN GENERAL.—A person, including a health care provider, health researcher, health plan, health or life insurer, medical or health savings plan administrator, school or university, health care clearinghouse, health oversight agency, public health authority, employer, or data broker, or such person’s agent, officer, employee, or affiliate, that accesses,
maintains, retains, modifies, records, stores, or other-
wise holds, uses, or discloses protected health in-
formation, shall permit an individual who is the sub-
ject of such protected health information, or the in-
dividual’s designee, to inspect and copy the protected
health information concerning the individual, includ-
ing records created under sections 102, 112, 202,
203, and 211.

(2) PROCEDURES AND FEES.—A person de-
scribed in paragraph (1) may establish appropriate
procedures to be followed for inspection and copying
under such paragraph and may require an individual
to pay reasonable fees associated with such inspec-
tion 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 person described in subsection
(a)(1) shall comply with a request for inspection or copy-
ing of protected 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 re-
quires 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 Sec-
etary determines appropriate, if such request re-
quires only the inspection, copying, or sending of
electronic or other digital materials.

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

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

(2) the person has been asked by the person de-
scribed in subsection (a)(1) to fulfill the require-
ments of this section.

(d) Special Rule Relating to Ongoing Clinical
Trials.—With respect to protected health information
that is created as part of an individual’s participation in
an ongoing clinical trial, access to the information shall
be provided consistent with the individual’s agreement to
participate in the clinical trial.
SEC. 103. MODIFICATIONS TO PROTECTED HEALTH INFORMATION.

(a) In General.—Not later than 15 business days, or earlier if the Secretary determines appropriate, after the date on which a person described in section 102(a)(1) receives from an individual a request in writing to supplement, correct, amend, segregate, or remove protected health information concerning the individual, such person—

(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 person described in subsection (a) declines to make the modification requested under such subsection within 15 business days after receipt of such request, such person shall inform the individual 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 concerning the individual.

(c) Statement of Disagreement.—If an individual has filed with a person a statement of disagreement under subsection (b)(3), the person, in any subsequent disclosure of the disputed portion of the information—

(1) shall include, at the individual’s request, a copy of the individual’s statement in the individual’s health record set; and

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

(d) Rules Governing Agents.—A person that is the agent of a person described in subsection (a) shall only be required to make a modification to protected health information where—

(1) the protected health information is retained, distributed, used, or maintained by the agent; and
(2) the agent has been asked by such person to fulfill the requirements of this section.

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

(1) notify individuals whose records have been affected;

(2) notify persons and the agents of persons that receive, access, maintain, retain, modify, record, store, destroy, or otherwise use or disclose such data; and

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

SECTION 104. NOTICE OF PRIVACY PRACTICES.

(a) Preparation of Written Notice.—A person described in section 102(a)(1) shall prepare a written notice of the privacy practices of such person, including information with respect to the following:

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

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

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

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

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

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

(7) The right of and procedures for an indi-
vidual to request segregation of protected health in-
formation, and to restrict the use of such informa-
tion by employees, agents, and contractors of a person.

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

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

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

(11) The right of and procedures for an individual to request that protected health information be transferred to a third party person without unreasonable delay.
(12) The right to prompt notification of an actual or suspected security breach of protected health information, and how such breaches will be remedied by the person.

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

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

(b) PROVISION AND POSTING OF WRITTEN NOTICE.—

(1) PROVISION.—A person described in subsection (a) shall provide a copy of the written notice of privacy practices required under such subsection—

(A) at the time an authorization is sought for the disclosure of protected health information; and

(B) upon the request of an individual.
(2) POSTING.—A person described in subsection (a) 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 appointed under section 301, 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.

(d) REQUIREMENT FOR OPT-OUT.—A person shall not access, maintain, retain, modify, record, store, destroy, or otherwise use or disclose an individual’s protected health information for other than treatment or payment purposes until that individual has been given an opportunity, before the time that such information is initially used or disclosed, to direct that such information not be used or disclosed. The individual must be given adequate time to exercise the nondisclosure and nonuse option (referred to as the “opt-out”) through the method that is most convenient to the individual, along with an explanation of how the individual can exercise such option.
SEC. 105. DEMONSTRATION GRANT.

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

(b) PURPOSE.—It is the purpose of this section, to promote the cultural competency of persons that access, maintain, retain, modify, record, store, destroy, or otherwise use or disclose protected health information, and to enable such persons to better communicate privacy 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.

Subtitle B—Establishment of Safeguards

SEC. 111. ESTABLISHMENT OF SAFEGUARDS.

(a) IN GENERAL.—A person described in section 102(a)(1) shall establish and maintain appropriate administrative, organizational, technical, and physical safeguards and procedures to ensure the privacy, confidentiality, security, accuracy, and integrity of protected health
information that is accessed, maintained, retained, modified, recorded, stored, destroyed, or otherwise used or disclosed by such person.

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

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

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

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

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

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

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

(c) MODEL GUIDELINES.—The Secretary, in consultation with the Director of the Office of Health Information Privacy appointed under section 301, after notice and opportunity for public comment, shall develop and disseminate model guidelines for the establishment of safe-
guards and procedures for use under this section, such as, where appropriate, individual authentication of uses of computer systems, access controls, audit trails, encryption, physical security, protection of remote access points and protection of external electronic communications, periodic security assessments, incident reports, and sanctions. The Director shall update and disseminate the guidelines, as appropriate, to take advantage of new technologies.

(d) Review and Updating of Safeguards.—Persons subject to this Act 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 persons described in subsection (a), as appropriate.

SEC. 112. TRANSPARENCY.

(a) Public List of Data Brokers.—A person described in section 102(a)(1) shall establish a list of data brokers with which such person has entered into a contract or relationship for the purposes of providing services involving any protected health information. Such list and
the contact information for each broker shall be made publicly accessible on the Internet.

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

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

(2) require by contract that such service providers implement and maintain appropriate measures designed to meet the requirements of persons subject to this Act;

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

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

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

**SEC. 113. RISK MANAGEMENT.**

(a) **IN GENERAL.**—Persons described in section 102(a)(1) that have access to protected health information shall establish risk management and control processes to protect against anticipated vulnerabilities to the privacy, security, and integrity of protected health information.

(b) **RISK ASSESSMENT.**—A person described in subsection (a) shall perform annual risk assessments of procedures, systems, or networks involved in the creation, accessing, maintenance, retention, modification, recording, storage, distribution, destruction, or other use or disclosure of personal health information. Such risk assessment may include—

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

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

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

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

(c) RISK MANAGEMENT.—A person described in subsection (a) shall establish risk management and control procedures designed to control risks such as those identified in subsection (b). Such procedures shall include—

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

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

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

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

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

SEC. 114. ACCOUNTING FOR DISCLOSURES AND USE.

(a) In General.—A person described in section 102(a)(1) shall establish and maintain, with respect to any protected 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 7 years.

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

(d) ACCESS TO RECORDS.—A person described in
subsection (a) shall permit an individual who is the subject
of protected health information, or the individual’s des-
ignee, to inspect and copy the records created in para-
graphs (a) and (c) of this section.

TITLE II—RESTRICTIONS ON
USE AND DISCLOSURE
Subtitle A—General Restrictions
on Use and Disclosure

SEC. 201. GENERAL RULES REGARDING USE AND DISCLOSURE.

(a) Prohibition.—

(1) General rule.—A person may not dis-
close, access, or use protected health information ex-
cept as authorized under this Act.

(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 protected health information.

(b) Scope of Disclosure or Use.—

(1) In general.—A disclosure or use of protected health information under this title shall be limited to the minimum amount of information necessary to accomplish the purpose for which the disclosure or use is made.

(2) Determination.—The determination as to what constitutes the minimum disclosure or use possible for purposes of paragraph (1) shall be made by a health care provider to the extent required by law. The minimum necessary standard is intended to be consistent with, and not override, professional judgment and standards.

(c) Use or Disclosure for Purpose Only.—An authorized recipient of information pursuant to this title may use or disclose such information solely to carry out the purpose for which the information was disclosed, except as provided in section 214.

(d) No General Requirement To Disclose.—Nothing in this title permitting the disclosure of protected health information shall be construed to require such disclosure.
(c) **Identification of Disclosed Information as Protected Health Information.**—Protected health information disclosed or used pursuant to this title shall be clearly identified and labeled as protected health information that is subject to this Act.

(f) **Disclosure or Use by Agents.**—An agent, employee, or affiliate of a person described in section 102(a)(1) that accesses, seeks to access, obtains, discloses, uses, or receives protected health information from such person, shall be subject to this title to the same extent as the person.

(g) **Disclosure or Use by Others.**—A person receiving protected health information initially held by a person described in subsection (f) shall be subject to this title 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 protected 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 or other secondary or tertiary means for
accessing protected health information shall be deemed to
be a disclosure of protected health information. The unau-
alyzed use of a decryption key (or other secondary or
tertiary means for accessing protected health information)
or de-identified health information in order to identify an
individual is deemed to be disclosure of protected health
information.

(j) NO WAIVER.—Except as provided in this Act, an
authorization to disclose or use personally identifiable
health information executed by an individual pursuant to
section 202 or 203 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-OUT.—A person may not disclose, access, or
use an individual’s protected health information until that
individual has been given the opportunity to opt out of
any local, regional, or nationwide health information net-
work or system that is used by the person.

(l) DISPOSAL OF DATA.—To prevent the unauthor-
ized disclosure or use of protected health information,
such information, when disposed of, shall be fully de-iden-
tified, destroyed, and expunged from any electronic, paper,
or other files and documents maintained by authorized
persons.
(m) Obligations of Unauthorized Recipients.—A person that obtains, accesses, or receives protected 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 protected health information under such circumstances shall be deemed an unauthorized disclosure of protected health information.

(n) Definitions.—In this title:

(1) Investigative or law enforcement officer.—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.

(2) Segregate.—The term “segregate” means to hide, mask, or mark separate a designated subset of an individual’s protected health information, or to place such a subset in a location that is securely separated from the location used to store other protected 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.

(3) **Signed.**—The term “signed” refers to both signatures in ink and electronic signatures, and the term “written” refers to both paper and computerized formats.

**SEC. 202. INFORMED CONSENT FOR DISCLOSURE OF PROTECTED 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.**—To satisfy the requirement under section 201(b)(1), an employer, health plan, health or life insurer, or health care provider that seeks to disclose protected health information in connection with treatment or payment shall obtain an authorization from the subject of such protected health information that satisfies the requirements of this section. A single authorization may authorize multiple disclosures.

(2) **Employers.**—Every employer offering a health plan to its employees shall, at the time of an employee’s enrollment in the health plan, obtain a
signed, written authorization that is an authorization based on informed consent that satisfies the requirements of subsection (b) concerning the use and disclosure of protected health information for treatment or payment with respect to each individual who is eligible to receive care under the health plan.

(3) 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 a signed, written authorization that is a legal, informed authorization that satisfies the requirements of subsection (b) concerning the use and disclosure of protected health information with respect to each individual who is eligible to receive care or benefits under the plan or insurance.

(4) 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 a signed, written authorization that satisfies the requirements of subsection (b) to access or use protected health information in providing health care or arranging for health care from other providers or seeking payment for the provision of health care services.
(5) Providers.—

(A) In General.—Every health care provider that provides health care to an individual that has not been given the appropriate prior authorization under this section, shall at the time of providing such care obtain a signed, written authorization that is a legal, informed authorization, that satisfies the requirements of subsection (b), concerning the use and disclosure of protected health information with respect to such individual.

(B) Rule of Construction.—Subparagraph (A) shall not be construed to preclude the provision of health care to an individual who has not given appropriate authorization prior to receipt of such care if—

(i) the health care provider involved determines that such care is essential; and

(ii) the individual can reasonably be expected to sign an authorization for such care when appropriate.

(b) Requirements for Individual Informed Consent.—To satisfy the requirements of this subsection, an authorization from an individual to disclose the individual’s protected 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, or operating within, a person authorized to disclose the information;

(2) describe the 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, or operating within, 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 authorization is not authorized to receive protected 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 protected 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 authorization is valid until revocation by the individual or until an event or date specified;

(8)(A) be—

(i) in writing, dated, and signed by the individual; or

(ii) in electronic form, dated and authenticated by the individual using an authentication method approved by the Secretary; and

(B) not have been revoked under subparagraph (A);

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

(10) include a concise description of any systems or services used for access, maintenance, retention, modification, recording, storage, destruction, or other use of protected health information by the authorized person, including—

(A) a description of any linkages made with other systems, databases, networks, or services external to the authorized person; and
(B) how the linkages made with other systems, databases, networks, or services external to the authorized person meet the privacy and security standards of the authorized person;

(11) 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 protected health information to a sub-contracted person operating or located overseas; and

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

(c) LIMITATION ON AUTHORIZATIONS.—

(1) IN GENERAL.—Subject to paragraphs (2) and (3), a person described in section 102(a)(1) that seeks an authorization under this title may not condition the delivery of treatment or payment for services on the receipt of such an authorization.

(2) RIGHT TO REQUIRE SELF-PAYMENT.—If an individual has refused to provide an authorization
for disclosure of administrative billing information to
a person and such authorization 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 serv-
ices.

(3) **Right of Health Care Provider to Re-
quire Authorization for Treatment Pur-
poses.**—If a health care provider that is seeking an
authorization for disclosure of an individual's pro-
tected health information believes that the disclosure
of such information is necessary so as not to endan-
ger 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 con-
dition the provision of services upon the individual's
execution of an authorization to disclose personal
health information to the minimum extent necessary.

(4) **Authorizations 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 pro-
tected health information and no other arrange-
ments have been made to pay for the health care
services being rendered to the patient, such informa-
tion may be disclosed to a governmental authority to
the extent necessary to determine the individual’s
eligibility for, and to obtain, payment under a gov-
ernmental 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 pay-
ment for health care services rendered by that pro-
vider of health care or health care service plan to the
patient.

(d) MODEL AUTHORIZATIONS.—The Secretary, in
consultation with the Director of the Office of Health In-
formation Privacy, after notice and opportunity for public
comment, shall develop and disseminate model written au-
thorizations of the type described in this section and model
statements of the limitations on authorizations. Any au-
thorization obtained on a model authorization form under
section 202 developed by the Secretary pursuant to the
preceding sentence shall be deemed to satisfy the require-
ments of this section.

(e) SEGREGATION OF FILES.—A person described in
section 102(a)(1) shall comply with the request of an indi-
vidual who is the subject of protected health information—
(1) to hide, mask, or mark separate any type or amount of protected 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 protected health information.

(f) REVOCATION OF AUTHORIZATION.—

(1) IN GENERAL.—An individual may, electronically or in writing, revoke or amend an authorization under this section at any time, unless the disclosure that is the subject of the authorization 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 PLANS.—With respect to a health plan, the authorization 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.
(3) ACTIONS.—An individual may not maintain an action against a person for disclosure of personally identifiable health information—

(A) if the disclosure was made based on a good faith reliance on the individual’s authorization under this section at the time such disclosure was made;

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

(C) if the disclosure was for the purpose of protecting another individual from imminent physical harm, and is authorized under section 204.

(g) RECORD OF INDIVIDUAL’S AUTHORIZATIONS AND REVOCATIONS.—Each person accessing, maintaining, retaining, modifying, recording, storing, destroying, or otherwise using personally identifiable or protected health information shall maintain a record for a period of 7 years of each authorization by an individual and any revocation thereof, and such record shall become part of the individual’s health record set.

(h) RULE OF CONSTRUCTION.—Authorizations for the disclosure of protected health information for treatment or payment shall not authorize the disclosure of such
information where the intent is to sell, market, transfer, or use the protected health information for a commercial advantage other than for the revenues directly derived from the provision of health care to that individual. With respect to such a disclosure for a use other than for treatment or payment, a separate authorization that satisfies the requirements of section 203 is required.

SEC. 203. AUTHORIZATIONS FOR DISCLOSURE OF PROTECTED HEALTH INFORMATION OTHER THAN FOR TREATMENT OR PAYMENT.

(a) IN GENERAL.—To satisfy the requirement under section 201(b)(1), a health care provider, health plan, health oversight agency, public health authority, employer, health researcher, law enforcement official, health or life insurer, school or university, or other person described under section 102(a)(1) that seeks to disclose protected health information for a purpose other than treatment or payment shall obtain an authorization that satisfies the requirements of subsections (b), (e), (f), and (g) of section 202. Such an authorization under this section shall be separate from an authorization provided under section 202.

(b) LIMITATION ON AUTHORIZATIONS.—

(1) IN GENERAL.—A person subject to section 202 may not condition the delivery of treatment, or
payment for services, on the receipt of an authorization described in this section.

(2) **Requirement for separate authorization.**—A person subject to section 202 may not disclose protected 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 authorization permitting such a disclosure.

(c) **Model Authorizations.**—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 written authorizations of the type described in subsection (a). Any authorization obtained on a model authorization form under this section shall be deemed to meet the authorization requirements of this section.

(d) **Requirement to Release Protected Health Information to Coroners and Medical Examiners.**—

(1) **In general.**—When a coroner or medical examiner or their duly appointed deputies seek protected health information for the purpose of inquiry into and determination of, the cause, manner, and
circumstances of an individual’s death, the health
care provider, health plan, health oversight agency,
public health authority, employer, health researcher,
law enforcement officer, health or life insurer, school
or university, or other person involved shall provide
that individual’s protected health information to the
coroner or medical examiner or to the duly ap-
pointed deputies without undue delay.

(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 protected health
information unless the health information is at-
tached 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 med-
ical examiner’s official report shall be exempt from
the provisions of this Act except as provided for in
this subsection.

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

(e) Revocation or Amendment of Authorization.—An individual may, in writing, revoke or amend an authorization under this section at any time.

(f) Actions.—An individual may not maintain an action against a person described in section 102(a)(1) for the disclosure of protected health information—

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

(2) in a case in which the 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 204.

(g) Record of Authorizations and Revocations.—Each person accessing, maintaining, retaining, modifying, recording, storing, destroying, or otherwise using personally identifiable or protected health information for purposes other than treatment or payment shall maintain a record for a period of 7 years of each authorization by an individual and any revocation thereof, and
such record shall become part of the individual’s health record set.

SEC. 204. NOTIFICATION IN THE CASE OF BREACH.

(a) In General.—A person described in section 102(a)(1) that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise uses or discloses protected health information shall, following the discovery of a security breach of such information, notify each individual whose protected 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 protected 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 protected health information.
information subject to the security breach, to pro-
vide 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 protected health information sub-
ject to the security breach, or other designated third
party, provides such notification.

(e) 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 se-
curity 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 protected health information of more than 1,000 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 persons described in section 102 (a)(1) that have lost, stolen, disclosed, or used in an unauthorized manner or for an unauthorized purpose the protected health information of a significant number of individuals.

(e) CONTENT OF NOTIFICATION.—Regardless of the method by which notice is provided to individuals under
section 104, notice of a security breach shall include, to
the extent possible—

(1) a description of the protected health infor-
mation 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 protected health information
the person maintained about that individual; and

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

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

(1) IN GENERAL.—If a Federal law enforce-
ment agency determines that the notification re-
quired under this section would impede a criminal
investigation or cause damage to national security,
such notification shall be delayed upon written no-
tice 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 de-
layed pursuant to paragraph (1), a person shall give
notice not later than 30 days after such law enforce-
ment delay was invoked unless a Federal law enforcement agency provides written notification that further delay is necessary.

(3) LAW ENFORCEMENT IMMUNITY.—No cause of action shall arise in any court against any Federal law enforcement agency for acts relating to the delay of notification for law enforcement purposes under this subtitle.

Subtitle B—Disclosure Under Special Circumstances

SEC. 211. EMERGENCY CIRCUMSTANCES.

(a) GENERAL RULE.—In the event of a threat of imminent physical or mental harm to the subject of protected health information, any person may, in order to allay or remedy such threat, disclose protected 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 protected 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. 212. PUBLIC HEALTH.

(a) In General.—A health care provider, health plan, public health authority, employer, health or life insurer, law enforcement official, school or university, or other person described in section 102(a)(1) may disclose protected health information to a public health authority 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 protection” means a population-based activity or individual effort, authorized by law, the purpose of which is the preven-
tion of injury, disease, or premature mortality, or the pro-
motion 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 emer-
gencies; and

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

(c) LIMITATIONS.—The purpose of the disclosure de-
scribed in subsection (a) should be of sufficient importance
to warrant the potential effect on, or risk to, the privacy
of individuals that the additional exposure of protected
health information might bring. Any infringement on the
right to privacy under this section should use the least
intrusive means that are tailored to minimize intrusion on
the right to privacy.

SEC. 213. PROTECTION AND ADVOCACY AGENCIES.

Any person described in section 102(a)(1) that cre-
ates, accesses, maintains, retains, modifies, records,
stores, destroys, or otherwise uses or discloses protected
health information under this title may disclose such infor-
mation 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 can establish that there is probable cause to believe that an individual who is the subject of the protected health information is vulnerable to abuse and neglect by an entity providing health or social services to the individual.

SEC. 214. OVERSIGHT.
(a) IN GENERAL.—A health care provider, health plan, employer, law enforcement official, health or life insurer, public health authority, health researcher, school or university, or other person described in section 102(a)(1) may disclose protected health information to a health oversight agency 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 protected 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 PROTECTED HEALTH INFORMATION.—A health oversight agency that receives protected health information under this section—

(1) shall secure protected health information in all work papers and all documents summarizing the health oversight activity through technological, administrative, and physical safeguards including cryptographic-key based encryption;

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

(3) 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

(4) shall remove or destroy the information that allows subjects of protected 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) **Use of Protected Health Information in Judicial Proceedings.**—

(1) **In General.**—The disclosure and use of protected health information in any judicial, administrative, court, or other public proceeding or investigation relating to a health oversight activity shall be undertaken in such a manner as to preserve the confidentiality and privacy of individuals who are the subject of the information, unless disclosure is required by the nature of the proceedings.

(2) **Limiting Disclosure.**—Whenever disclosure of the identity of the subject of protected health information is required by the nature of the proceedings, or it is impracticable to redact the identity of such individual, the agency shall request that the presiding judicial or administrative officer enter an order limiting the disclosure of the identity of the subject to the extent possible, including the redacting of the protected health information from publicly disclosed or filed pleadings or records.

(d) **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 protected health information is being sought for a legally authorized oversight function.

(c) Use in Action Against Individuals.—Protected health information about an individual that is disclosed under this section may not be used in, or disclosed to any person for use in, an administrative, civil, or criminal action or investigation directed against the individual, unless the action or investigation arises out of and is directly related to—

(1) the receipt of health care or payment for health care;

(2) a fraudulent claim related to health; or

(3) oversight of a public health authority or a health researcher.

SEC. 215. DISCLOSURE FOR LAW ENFORCEMENT, NATIONAL SECURITY, AND INTELLIGENCE PURPOSES.

(a) Access to Protected Health Information for Law Enforcement, National Security, and Intelligence Activities.—A person described in section 102(a)(1), or a person who receives protected health information pursuant to section 211, may disclose protected health information to—

(1) an investigative or law enforcement officer 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) Requirements for Court Orders for Access to Protected Health Information.—A court order for the disclosure of protected health information under subsection (a)(1) may be issued by any court that is a court of competent jurisdiction and shall issue only if the investigative or law enforcement officer submits a written application upon oath or equivalent affirmation demonstrating that there is probable cause to believe that—

(1) the protected health information sought is relevant and material to an ongoing criminal investigation, except in the case of a State government authority, such a court order shall not issue if prohibited by the law of such State;
(2) the investigative or evidentiary needs of the investigative or law enforcement officer cannot reason-ably be satisfied by de-identified health informa-
tion or by any other information; and

(3) the law enforcement need for the informa-
tion outweighs the privacy interest of the individual to whom the information pertains.

(c) Motions To Quash Or Modify.—A court issuing an order pursuant to this section, on a motion made promptly by a person described in subsection (a)(1) may quash or modify such order if the court finds that information or records requested are unreasonably volumi-
nous or if compliance with such order otherwise would cause an unreasonable burden on such entities.

(d) Notice.—

(1) In General.—Except as provided in para-
graph (2), no order for the disclosure of protected health information about an individual may be issued by a court under this section unless prior no-
tice of the application for the order has been served on the individual and the individual has been af-
forded an opportunity to oppose the issuance of the order.

(2) Notice Not Required.—An order for the disclosure of protected health information about an
individual may be issued without prior notice to the
individual if the court finds that notice would be im-
practical because—

(A) the name and address of the individual
are unknown; or
(B) notice would risk destruction or un-
availability of the evidence, intelligence,
counter-intelligence, or other national security
information.

(c) CONDITIONS.—Upon the granting of an order for
disclosure of protected health information under this sec-
tion, the court shall impose appropriate safeguards to en-
sure the confidentiality of such information and to protect
against unauthorized or improper use or disclosure.

(f) LIMITATION ON USE AND DISCLOSURE FOR NA-
TIONAL SECURITY, INTELLIGENCE, AND OTHER LAW EN-
FORCEMENT INQUIRIES.—Protected 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 investiga-
tion 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.
(g) **DESTRUCTION OR RETURN OF INFORMATION.**—When the matter or need for which protected health information was disclosed to an investigative or law enforcement officer, a Federal official authorized for the conduct of lawful intelligence, counter-intelligence, and other national security activities, or authorized Federal official, or grand jury has concluded, including any derivative matters arising from such matter or need, the law enforcement agency, authorized Federal official, or grand jury shall either destroy the protected health information, or return it to the entity from which it was obtained.

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

(i) **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.

**SEC. 216. NEXT OF KIN AND DIRECTORY INFORMATION.**

(a) **NEXT OF KIN.**—A health care provider, or a person that receives protected health information under section 211, may disclose protected 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.

SEC. 217. 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 enactment of this Act, the Secretary shall prepare and submit to Congress detailed recommendations on whether written informed consent should be required, and if so, under what circumstances, before protected 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 summary of how technology could be used to strip identifying data for the purposes of research;

(3) an analysis of the risks and benefits of requiring informed consent versus the waiver of informed consent;

(4) an analysis of the risks and benefits of using protected health information for research purposes other than the health research project for which such information was obtained; 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, 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 protected 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; and
(B) 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 re-
search under this section shall provide the Sec-
retary with the names and addresses of the in-
stitutional review board members.

(B) Technical assistance.—The Sec-
retary shall provide technical assistance to insti-
tutional review boards described in this sub-
section.

(C) Monitoring.—The Secretary shall pe-
riodically monitor institutional review boards
described in this subsection.

(D) Reports.—Not later than 3 years
after the date of enactment of this Act, the Sec-
retary shall report to Congress regarding the
activities of institutional review boards de-
scribed in this subsection.

(g) Limitation.—Nothing in this section shall be
construed to permit protected 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 protected health in-
formation.

SEC. 218. JUDICIAL AND ADMINISTRATIVE PURPOSES.

(a) IN GENERAL.—A person described in section
102(a)(1), or a person who receives protected health infor-
mation under section 211, may disclose protected health
information—

(1) pursuant to the standards and procedures
established in the Federal Rules of Civil Procedure
or comparable rules of other courts or administrative
agencies, in connection with litigation or proceedings
to which an individual who is the subject of the in-
formation is a party and in which the individual has
placed his or her physical or mental condition at
issue;

(2) to a court, and to others ordered by the
court, if in response to a court order issued by a
court of competent jurisdiction in accordance with
subsections (b) and (c); or

(3) if necessary to present to a court an appli-
cation regarding the provision of treatment of an in-
dividual or the appointment of a guardian.

(b) COURT ORDERS FOR ACCESS TO PROTECTED
HEALTH INFORMATION.—A court order for the disclosure
of protected health information under subsection (a) may be issued only if the person seeking disclosure submits a written application upon oath or equivalent affirmation demonstrating by clear and convincing evidence that—

(1) the protected health information sought is necessary for the adjudication of a material fact in dispute in a civil proceeding;

(2) the adjudicative need cannot be reasonably satisfied by de-identified health information or by any other information; and

(3) the need for the information outweighs the privacy interest of the individual to whom the information pertains.

(e) NOTICE.—

(1) IN GENERAL.—Except as provided in paragraph (2), no order for the disclosure of protected health information about an individual may be issued by a court unless notice of the application for the order has been served on the individual and the individual has been afforded an opportunity to oppose the issuance of the order.

(2) NOTICE NOT REQUIRED.—An order for the disclosure of protected health information about an individual may be issued without notice to the indi-
individual if the court finds, by clear and convincing evi-
dence, that notice would be impractical because—

(A) the name and address of the individual
are unknown; or

(B) notice would risk destruction or un-
availability of the evidence.

(d) OBLIGATIONS OF RECIPIENT.—A person seeking
protected health information pursuant to subsection
(a)(1)—

(1) shall notify the individual or the individual’s
attorney of the request for the information;

(2) shall provide the health care provider,
health plan, health oversight agency, employer, in-
surer, health or life insurer, school or university,
agent, or other person involved with a signed docu-
ment attesting—

(A) that the individual has placed his or
her physical or mental condition at issue in liti-
gation or proceedings in which the individual is
a party; and

(B) the date on which the individual or the
individual’s attorney was notified under para-
graph (1); and

(3) shall not accept any requested protected
health information from the health care provider,
health plan, health oversight agency, employer, insurer, health or life insurer, school or university, agent, or other person until the termination of the 10-day period beginning on the date notice was given under paragraph (1).

SEC. 219. 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 Act.

(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 Act to the extent necessary to effectuate the terms or purposes of the grant of authority.

(c) NO COURT DECLARATION.—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 Act may be exercised and discharged in the best inter-
est of the individual by—

(1) a person described in subsection (b) with re-
spect to the individual;

(2) a person described in subsection (a) with re-
spect to the individual, but only if a person de-
scribed 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 per-
son 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 CA-
PABLE.—In the case of an individual—

(A) who is 18 years of age or older, all
rights of the individual under this Act 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 Act with respect to protected 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 Act 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 protected 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.
(c) **DECEASED INDIVIDUALS.**—

(1) **APPLICATION OF ACT.**—The provisions of this Act shall continue to apply to protected 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 Act. 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 216(a) may disclose protected health information if such disclosure is necessary to assist in the identification of a deceased individual.
TITLE III—OFFICE OF HEALTH INFORMATION PRIVACY OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES

Subtitle A—Designation

SEC. 301. DESIGNATION.

(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 Act;

(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 Act (and the regulations promulgated under this Act);
(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 protected health information and concerning medical privacy research needs; and

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

(e) 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 used to access, disclose, maintain, store, distribute, transmit, amend, or dispose of protected 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 tech-
ology and information systems, and experts in health care.

(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 consultation with the Director of the Office, shall prepare and submit to Congress a report concerning the number of complaints of alleged violations of this Act 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.

Subtitle B—Enforcement

CHAPTER 1—CRIMINAL PROVISIONS

SEC. 311. WRONGFUL DISCLOSURE OF PROTECTED HEALTH INFORMATION.

(a) IN GENERAL.—Part I of title 18, United States Code, is amended by adding at the end the following:
“CHAPTER 124—WRONGFUL DISCLOSURE
OF PROTECTED HEALTH INFORMATION

“SEC. 2801. WRONGFUL DISCLOSURE OF PROTECTED
HEALTH INFORMATION.

“(a) OFFENSE.—The penalties described in sub-
section (b) shall apply to a person that knowingly and in-
tentionally—

“(1) obtains, uses, or attempts to obtain or use
protected health information relating to an indi-
vidual in violation of title II of the Health Informa-
tion Privacy and Security Act; or

“(2) discloses or attempts to disclose protected
health information to another person in violation of
title II of the Health Information Privacy and Secu-
rity Act.

“(b) PENALTIES.—A person described in subsection
(a) shall—

“(1) be fined not more than $50,000, impris-
oned not more than 1 year, or both;

“(2) if the offense is committed under false pre-
tenses, be fined not more than $250,000 or impris-
oned not more than 5 years, or both; or

“(3) if the offense is committed with the intent
to sell, transfer, or use protected health information
for commercial advantage, personal gain, or mali-
cious harm, be fined not more than $500,000, im-
prisoned not more than 10 years, or any combina-
tion of such penalties.

“(c) SUBSEQUENT OFFENSES.—In the case of a per-
son described in subsection (a), the maximum penalties
described in subsection (b) shall be doubled for every sub-
sequent conviction for an offense arising out of a violation
or violations related to a set of circumstances that are dif-
ferent from those involved in the previous violation or set
of related violations described in such subsection (a).”.

(b) CLERICAL AMENDMENT.—The table of chapters
for part I of title 18, United States Code, is amended by
inserting after the item relating to chapter 123 the fol-
lowing new item:

“Sec. 2801. Wrongful disclosure of protected health information.”.

SEC. 312. DEBARMENT FOR CRIMES AND CIVIL VIOLA-
TIONS.

(a) PURPOSE.—The purpose of this section is to pre-
vent and deter instances of intentional criminal actions
that violate criminal laws that are designed to protect the
privacy of protected health information in a manner con-
sistent with this Act.

(b) DEBARMENT.—Not later than 270 days after the
date of enactment of this Act, the Attorney General, in
consultation with the Secretary, shall promulgate regula-
tions and establish procedures to permit the debarment
of health care providers, health researchers, health or life
insurers, employers, or schools or universities from receiving benefits under any Federal health program or other
Federal procurement program if the managers or officers
of such persons are found guilty of violating section 2801
of title 18, United States Code, have civil penalties im-
posed against such officers or managers under section 321
in connection with the illegal disclosure of protected health
information, or are found guilty of making a false state-
ment or obstructing justice related to attempting to con-
ceal or concealing such illegal disclosure. Such regulations
shall take into account the need for continuity of medical
care and may provide for a delay of any debarment im-
posed under this section to take into account the medical
needs of patients.

(e) Consultation.—Prior to publishing a proposed
rule to implement subsection (b), the Attorney General
shall consult with State law enforcement officials, health
care providers, patient privacy rights’ advocates, and other
appropriate persons, to gain additional information re-
grading the debarment of persons under subsection (b)
and the best methods to ensure the continuity of medical
care.

(d) Report.—The Attorney General shall annually
prepare and submit to the Committee on the Judiciary of
the House of Representatives and the Committee on the Judiciary of the Senate a report concerning the activities and debarment actions taken by the Attorney General under this section.

(e) Assistance To Prevent Criminal Violations.—The Attorney General, in cooperation with any other appropriate individual, organization, or agency, may provide advice, training, technical assistance, and guidance regarding ways to reduce the incidence of improper disclosure of protected health information.

(f) Relationship to Other Authorities.—A debarment imposed under this section shall not reduce or diminish the authority of a Federal, State, or local governmental agency or court to penalize, imprison, fine, suspend, debar, or take other adverse action against a person, in a civil, criminal, or administrative proceeding.

CHAPTER 2—CIVIL SANCTIONS

SEC. 321. CIVIL PENALTY.

A health care provider, health researcher, health plan, health oversight agency, public health agency, law enforcement agency, employer, health or life insurer, school or university, agent or other person described in section 102(a)(1), who the Secretary, in consultation with the Attorney General, determines has substantially and materially failed to comply with this Act 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 title I, 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 title II, 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.

SEC. 322. PROCEDURES FOR IMPOSITION OF PENALTIES.

(a) INITIATION OF PROCEEDINGS.—The Attorney General, in consultation with the Secretary, may initiate a proceeding in United States District Court to recover a civil money penalty under section 321. The Attorney General may not initiate an action under this section with respect to any violation described in section 321 after the expiration of the 6-year period beginning on the date on which such violation was alleged to have occurred. The Attorney General may initiate an action under this section
by filing a complaint pursuant to Rule 4 of the Federal
Rules of Civil Procedure.

(b) Scope of Penalty.—In determining the
amount or scope of any penalty sought pursuant to section
321, the Attorney General shall take into account—

(1) the nature of claims and the circumstances
under which they were presented;

(2) the degree of culpability, history of prior of-
fenses, and financial condition of the person against
whom the claim is brought; and

(3) such other matters as justice may require.

(c) Recovery of Penalties.—

(1) In general.—Civil money penalties im-
posed under this section may be recovered in a civil
action in the name of the United States brought in
United States district court for the district where
the claim was presented, or where the claimant res-
sides, as determined by the Attorney General.
Amounts recovered under this section shall be paid
to the United States and deposited as miscellaneous
receipts of the Treasury of the United States.

(2) Deduction from amounts owing.—The
amount of any penalty may be deducted from any
sum then or later owing by the United States or a
State to the person against whom the penalty has been assessed.

(d) INJUNCTIVE RELIEF.—Whenever the Attorney General in consultation with the Secretary has reason to believe that any person has engaged, is engaging, or is about to engage in any activity which makes the person subject to a civil monetary penalty under section 321, the Attorney General may bring an action in an appropriate district court of the United States (or, if applicable, a United States court of any territory) to enjoin such activity, or to enjoin the person from concealing, removing, encumbering, or disposing of assets which may be required in order to pay a civil monetary penalty if any such penalty were to be imposed or to seek other appropriate relief.

(e) AGENCY.—A principal is jointly and severally liable with the principal’s agent for penalties under section 321 for the actions of the principal’s agent acting within the scope of the agency.

SEC. 323. CIVIL ACTION BY INDIVIDUALS.

(a) IN GENERAL.—Any individual whose rights under this Act have been knowingly or negligently violated may bring a civil action to recover—

(1) such preliminary and equitable relief as the court determines to be appropriate; and
(2) the greater of compensatory damages or liquidated damages of $5,000.

(b) PUNITIVE DAMAGES.—In any action brought under this section in which the individual has prevailed because of a knowing violation of a provision of this Act, the court may, in addition to any relief awarded under subsection (a), award such punitive damages as may be warranted.

c) ATTORNEY’S FEES.—In the case of a civil action brought under subsection (a) in which the individual has substantially prevailed, the court may assess against the respondent a reasonable attorney’s fee and other litigation costs and expenses (including expert fees) reasonably incurred.

(d) LIMITATION.—No action may be commenced under this section more than 3 years after the date on which the violation was or should reasonably have been discovered.

(e) AGENCY.—A principal is jointly and severally liable with the principal’s agent for damages under this section for the actions of the principal’s agent acting within the scope of the agency.

(f) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—An action shall be brought under subsection (a) 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; and

(B) may be found.

(g) 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. 324. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) IN GENERAL.—

(1) CIVIL ACTIONS.—In any case in which the
attorney general of a State or any State or local law
enforcement 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 engage-
ment of a person in a practice that is prohibited
under this subtitle, the State or local law enforce-
ment agency on behalf of the residents of the agen-
cy’s jurisdiction, may bring a civil action on behalf
of the residents of the State or jurisdiction in a dis-

ctrict court of the United States of appropriate juris-
diction to—

(A) enjoin that act or practice;

(B) enforce compliance with this subtitle;

or

(C) obtain civil penalties of not more than

$1,000 per day per individual whose personally

identifiable information was, or is reasonably

believed to have been, accessed or acquired by

an unauthorized person, up to a maximum of

$50,000 per day.

(2) NOTICE.—

(A) IN GENERAL.—Prior to filing an ac-
tion under paragraph (1), the attorney general

of the State involved shall provide to the Attor-
ney General and Secretary—

(i) written notice of the action; and

(ii) a copy of the complaint for the ac-
tion.

(B) EXEMPTION.—Subparagraph (A) shall

not apply with respect to the filing of an action

by a State attorney general under this sub-
section, if the attorney general of a State deter-
mines that it is not feasible to provide the no-
tice described in this paragraph before the filing
of the action.

(C) Notification when practicable.—
In an action described under subparagraph (B),
the attorney general of a State shall provide the
written notice and a copy of the complaint to
the Attorney General and Secretary as soon
after the filing of the complaint as practicable.

(b) Federal Proceedings.—Upon receiving notice
under subsection (a)(2), the Attorney General in consulta-
tion with the Secretary, shall, have the right to—

(1) move to stay the action, pending the final
disposition of a pending Federal proceeding or ac-
tion;

(2) intervene in an action brought under sub-
section (a)(2); and

(3) file petitions for appeal.

(e) Pending Proceedings.—If the Attorney Gen-
eral has instituted a proceeding or action for a violation
of this subtitle or any regulations thereunder, no attorney
general of a State may, during the pendency of such pro-
ceeding or action, bring an action under this subtitle
against any defendant named in such criminal proceeding
or civil action for any violation that is alleged in that pro-
ceeding or action.
(d) **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.

(e) **Venue; Service of Process.**—

1. **Venue.**—Any action brought under sub-
   section (a) may be brought in the district court of
   the United States that meets applicable require-
   ments 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.

**SEC. 325. PROTECTION FOR WHISTLEBLOWER.**

(a) **Prohibition Against Discrimination.**—An
employer may not discharge, demote, suspend, threaten,
harass, retaliate against, or in any other manner discrimi-
nate or cause any employer to discriminate against an em-
ployee in the terms and conditions of employment because
of any lawful act committed by the employee to provide
information or cause information to be provided to a State
or Federal official relating to an actual or suspected viola-
tion of this Act by an employer or an employee of an em-
ployer.

(b) ENFORCEMENT ACTIONS.—

(1) IN GENERAL.—Any employee or former em-
ployee who alleges discharge or discrimination by
any person in violation of subsection (a) may seek
relief under subsection (c), by—

(A) filing a complaint with the Secretary of
Labor; or

(B) if the Secretary has not issued a final
decision within 180 days of the filing of the
complaint under subparagraph (A), and there is
no showing that such delay is due to the bad
faith of the claimant, bringing an action at law
or equity for de novo review in the appropriate
district court of the United States, which shall
have jurisdiction over such an action without
regard to the amount in controversy.

(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 an action brought under paragraph (1)(B).

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

(c) REMEDIES.—

(1) IN GENERAL.—If the district court determines in an action under subsection (b)(1) that a violation of subsection (a) has occurred, the court
shall order any relief necessary to make the employee whole.

(2) COMPENSATORY DAMAGES.—Relief in any action under subsection (b)(1) 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.

(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 
203(g)) for the purposes of implementing the re-
quirements 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 in-
cludes a public agency.

(g) GENERAL PROHIBITION AGAINST RETALIA-
tion.—A person described in section 102(a)(1), or any 
other person that receives protected health information 
under this title, may not adversely affect another person, 
directly or indirectly, because such person has exercised 
a right under this Act, disclosed information relating to 
a possible violation of this Act, or associated with, or as-
sisted, an individual in the exercise of a right under this 
Act.
TITLE IV—MISCELLANEOUS

SEC. 401. 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 protected health information or relating to an individual’s access to protected 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 in a court of the United States. Authorizations pursuant to section 202 shall not be construed as a waiver of any such privilege.

(e) 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 protected health information or health care services.

(d) FEDERAL PRIVACY ACT.—

(1) MEDICAL EXEMPTIONS.—Section 552a of title 5, United States Code, is amended by adding at the end the following:

“(w) CERTAIN PROTECTED HEALTH INFORMATION.—The head of an agency that is a health care provider, health plan, health oversight agency, employer, insurer, health or life insurer, school or university, or other entity who receives protected health information under section 218 of the Health Information Privacy and Security Act shall promulgate rules, in accordance with the requirements (including general notice) of subsections (b)(1), (b)(2), (b)(3), (c), (e) of section 553 of this title, to exempt a system of records within the agency, to the extent that the system of records contains protected health information (as defined in section 4 of such Act), from
all provisions of this section except subsections (b)(6), (d), (e)(1), (e)(2), subparagraphs (A) through (C) and (E) through (I) of subsection (e)(4), and subsections (e)(5), (e)(6), (e)(9), (e)(12), (l), (n), (o), (p), (r), and (u).”.

(2) TECHNICAL AMENDMENT.—Section 552a(f)(3) of title 5, United States Code, is amended by striking “pertaining to him,” and all that follows through the semicolon and inserting “pertaining to the individual”.

(e) 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 Act. The Secretary shall amend such Federal regulations as required to make such regulations consistent with this Act.

SEC. 402. EFFECTIVE DATE.

(a) EFFECTIVE DATE.—Unless specifically provided for otherwise, this Act 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 the promulgation of the regulations required under subsection (b).
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 Act.