To provide individuals with access to health information of which they are the subject, ensure personal privacy with respect to personal medical records and health care-related information, impose criminal and civil penalties for unauthorized use of personal health information, and to provide for the strong enforcement of these rights.

IN THE SENATE OF THE UNITED STATES

NOVEMBER 4, 1997

Mr. LEAHY (for himself and Mr. KENNEDY) introduced the following bill; which was read twice and referred to the Committee on Labor and Human Resources

A BILL

To provide individuals with access to health information of which they are the subject, ensure personal privacy with respect to personal medical records and health care-related information, impose criminal and civil penalties for unauthorized use of personal health information, and to provide for the strong enforcement of these rights.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the “Medical Information Privacy and Security Act”.


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

Sec. 1. Short title; table of contents.
Sec. 2. Findings.
Sec. 3. Purposes.
Sec. 4. Definitions.

TITLE I—INDIVIDUAL'S RIGHTS

Subtitle A—Access to Protected Health Information by Subjects of the
Information

Sec. 101. Inspection and copying of protected health information.
Sec. 102. Supplements to protected health information.
Sec. 103. Notice of privacy practices.

Subtitle B—Establishment of Safeguards

Sec. 111. Establishment of safeguards.
Sec. 112. Accounting for disclosures.

TITLE II—RESTRICTIONS ON USE AND DISCLOSURE

Subtitle A—General Restriction

Sec. 201. General rule regarding use and disclosure.

Subtitle B—Limited Circumstances Providing for Disclosure Without
Authorization

Sec. 211. Emergency circumstances.
Sec. 212. Public health.
Sec. 213. Protection and advocacy agencies.
Sec. 214. Oversight.
Sec. 215. Disclosure for law enforcement purposes.

Subtitle C—Special Rules Governing Disclosure

Sec. 221. Next of kin and directory information.
Sec. 222. Health research.
Sec. 223. Judicial and administrative purposes.
Sec. 224. Individual representatives.
Sec. 225. Prohibition against retaliation.

TITLE III—OFFICE OF HEALTH INFORMATION PRIVACY OF THE
DEPARTMENT OF HEALTH AND HUMAN SERVICES

Subtitle A—Establishment

Sec. 301. Establishment.

Subtitle B—Enforcement

CHAPTER 1—CRIMINAL PROVISIONS

Sec. 311. Wrongful disclosure of protected health information.
SEC. 2. FINDINGS.

Congress finds that—

(1) individuals have a right of privacy with respect to their personal medical information and records;

(2) with respect to information about medical care and health status, the traditional right of confidentiality (between a health care provider and a patient) is at risk;

(3) an erosion of the right of privacy may reduce the willingness of patients to confide in physicians and other practitioners and may inhibit such patients from seeking care;

(4) the use of electronic medical records offers many potential advantages compared to traditional paper-based systems if encompassed with strong privacy safeguards, through the sharing and linking of medical records electronically which can reduce costs, improve efficiencies and enhance medical care while helping to avoid duplicate tests, prevent fraud
and protect against unintended dangerous drug
interactions;

   (5) the European Union has adopted a directive
that provides that electronic medical records can not
be sent from Union member nations to other na-
tions, such as the United States, unless the non-
member country assures the security and confiden-
tiality of medical records under its national laws and
practices;

   (6) an individual’s privacy right means that the
individual’s consent is needed to disclose his or her
personally identifiable health information and that
the individual has a right of access to that health in-
formation;

   (7) any disclosure of personally identifiable
health information should be limited to that infor-
mation or portion of the medical record necessary to
fulfill the immediate and specific purpose of the dis-
closure;

   (8) an individual’s health information is cur-
rently accessible to many people who do not need the
information to provide health care to the individual,
often without the individual’s knowledge or consent;
(9) in the report of the National Research Council of March, 1997, the Council concluded that—

(A) with respect to the protection of electronic medical records, “few penalties exist for lax security” and that “few controls exist to prevent such information from being used in ways that could harm patients or invade their privacy”;

(B) “patients have little control over the ways in which information about their health is collected, used, or disseminated”;

(C) “[t]he greatest concerns regarding patient privacy stem from the widespread dissemination of information throughout the health care industry and related industries, often without the knowledge or consent of the patients . . . [i]n many cases, this information can be used in ways that are perceived as detrimental to patient privacy and contrary to the interests of patients. . . .”;  

(D) consent to release medical information should be for specified information and purposes and for limited amounts of time after
which the medical provider “must obtain new authorization from the patient”;

(E) “health care providers should give patients the right to request audits of all access to their electronic medical records and to review such logs”;

(F) with respect to the use of the social security number as a universal patient identifier, the “use of the social security number raises many legitimate privacy concerns”; and

(G) a national office of privacy should be established since “consumers need a mechanism for learning about their rights and how they may seek recourse for violations of fair information practices, and they need to be protected from the possibility that their access to care may be jeopardized by exercising their established privacy rights”;

(10) medical research often depends on access to both identifiable and nonidentifiable patient medical records and medical research is critically important to the health and well-being of all Americans;

(11) currently, there is technology available which can ease the process by which identifiable data can be stripped of all patient identifiers to sup-
port the necessary balance between medical research
and privacy protections for individuals;

(12) the American Medical Association Council
on Ethical Affairs has concluded that—

(A) a patient and a physician “should be
advised about the existence of computerized
data bases in which medical information con-
cerning the patient is stored”;

(B) information regarding the existence of
computerized data bases “should be commu-
nicated to the physician and patient prior to the
physician’s release of the medical information to
the entity or entities maintaining the computer
data bases”;

(C) a physician and patient “should be no-
tified of the distribution of all reports reflecting
identifiable patient data prior to distribution of
the reports by the computer facility”; and

(D) there should be “approval by the pa-
tient and notification of the physician prior to
the release of patient-identifiable clinical and
administrative data to individuals or organiza-
tions external to the medical care environment”;

(13)(A) genetic information contains the
uniquely private and personal genetic information of
an individual which is rapidly being deciphered and understood; and

(B) research in genetics continues to provide immense health benefits to individuals and their families, however, the improper use and unauthorized disclosure of genetic information may cause significant social and psychological harm to individuals, including stigmatization and discrimination;

(14) the Supreme Court found in Jaffee v. Redmond (116 S.Ct. 1923 (1996)) that—

(A) there is an imperative need for confidence and trust between a psychotherapist and a patient;

(B) this trust can only be established by an assurance of confidentiality; and

(C) preservation of such trust and confidentiality serves the public interest by facilitating the provision of appropriate treatment for individuals; and

(15) section 264 of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note) establishes a deadline that Congress enact legislation, within 36 months after the date of enactment of such Act, to protect the privacy of personal health information.
1 SEC. 3. PURPOSES.

2 It is the purpose of this Act to—

3 (1) recognize that there is a right to privacy 
4 with respect to health information, including genetic 
5 information, and that this right must be protected; 
6 (2) establish an Office of Health Information 
7 Privacy within the Department of Health and 
8 Human Services to protect that right of privacy; 
9 (3) provide individuals with—
10 (A) access to health information of which 
11 they are the subject; and 
12 (B) the opportunity to challenge the accu-
13 racy and completeness of such information by 
14 being able to file supplements of such records; 
15 (4) provide individuals with the right to limit 
16 the use and disclosure of personally identifiable 
17 health information; 
18 (5) create incentives to turn personal health in-
19 formation into nonidentifiable health information for 
20 oversight, health research, public health, law en-
21 forcement, judicial, and administrative purposes; 
22 (6) establish strong and effective mechanisms 
23 to protect against the unauthorized and inappropri-
24 ate use of personally identifiable health information 
25 that is created or maintained as part of health care
treatment, diagnosis, enrollment, payment, plan ad-
ministration, testing, or research processes;

(7) invoke the sweep of congressional powers,
including the power to enforce the 14th amendment,
to regulate commerce, and to abrogate the immunity
of the States under the 11th amendment, in order
to address violations of the rights of individuals to
privacy, to provide access to their medical records,
and to prevent unauthorized use of personal genetic
information; and

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

SEC. 4. 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 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 who represents and acts for another under the contract or relation of agency, or whose function is to bring about, modify, affect, accept performance of, or terminate contractual obligations between the principal and a third person, and includes the employees of such persons.

(3) DISCLOSE.—The term “disclose” means to release, transfer, permit access to, 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 redisclosures of individually identifiable health care information.

(4) EMPLOYER.—The term “employer” means a person engaged in business affecting commerce who has employees.

(5) 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;

and

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

(6) HEALTH CARE PROVIDER.—The term “health care provider” means a person, who with respect to a specific item of protected health information, receives, creates, uses, maintains, or discloses the information while acting in whole or in part in the capacity of—

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

(B) a Federal or State program that directly provides items or services that constitute health care to beneficiaries; or
(C) an officer or employee of a person described in subparagraph (A) or (B) that is engaged in the provision of health care.

(7) 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 of such person.

(8) Health Oversight Agency.—The term “health oversight agency” means a person who—

(A) 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

(B) 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 the assessment, evaluation, determination, investigation, or prosecution described in sub-
paragraph (A) and includes the employees of such person.

(9) **HEALTH PLAN.**—The term “health plan” means any health insurance plan, including any hospital or medical service plan, dental or other health service plan or health maintenance organization plan, or other program providing or arranging for the provision of health benefits, whether or not funded through the purchase of insurance. Such term includes employee welfare benefit plans and group plans as such plans are defined in sections 3 and 607 of the Employee Retirement Income Security Act of 1974 (29 U.S.C. 1002 and 1167).

(10) **HEALTH RESEARCHER.**—The term “health researcher” means a person who, with respect to a specific item of protected health information, receives the information—

(A) pursuant to section 222 (relating to health research); or

(B) while acting in whole or in part in the capacity of an officer or employee or agent of a person who receives the information described in subparagraph (A).

(11) **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.

(12) Nonidentifiable health information.—The term “nonidentifiable health information” means any information that would otherwise be protected health information except that it does not reveal the identity of the individual whose health or health care is the subject of the information and there is no reasonable basis to believe that the information could be used to identify that individual.

(13) Office of health information privacy.—The term “Office of Health Information Privacy” means the Office of Health Information Privacy established under section 301.

(14) Person.—The term “person” means a government, governmental subdivision of an executive branch agency or authority; corporation; company; association; firm; partnership; society; estate; trust; joint venture; individual; individual representative; tribal government; and any other legal entity.

(15) Protected health information.—The term “protected health information” means any information, including genetic information, demo-
graphic information, and tissue samples collected from an individual, whether oral or recorded in any form or medium, that—

(A) is created or received by a health care provider, health researcher, health plan, health oversight agency, public health authority, employer, health or life insurer, school or university; and

(B)(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)(I) identifies an individual; or

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

(16) 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.

(17) 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 learning, a college, or an assemblage of colleges united under one corporate organization or government.

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

(19) STATE.—The term “State” includes the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.

(20) WRITING.—The term “writing” means writing in either a paper-based or computer-based form, including electronic signatures.
TITLE I—INDIVIDUAL’S RIGHTS
Subtitle A—Access to Protected Health Information by Subjects of the Information

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

(a) Right of Individual.—

(1) In General.—A health care provider, health researcher, health plan, employer, health or life insurer, school, or university, or the agent of any such individual or entity, shall permit an individual who is the subject of protected health information, or the individual’s designee, to inspect and copy protected health information concerning the individual, including records created under sections 102 and 112, that such entity maintains.

(2) Procedures and Fees.—An entity described in paragraph (1) may set forth appropriate procedures to be followed for inspection and copying under such paragraph and may require an individual to pay fees associated with such inspection and copying in an amount that is not in excess of the actual costs of providing such copying. Such fees may not be assessed where such an assessment would have
the effect of prohibiting an individual from gaining
access to the information involved.

(b) DEADLINE.—An entity described in subsection
(a) shall comply with a request for inspection or copying
of protected health information under this section not
later than 15 business days after the date on which the
entity receives the request.

(c) RULES GOVERNING AGENTS.—An agent of an en-
tity described in subsection (a) shall provide for the in-
spection and copying of protected health information if—

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

(2) the agent has been asked by the entity in-
volved to fulfill the requirements of this section.

SEC. 102. SUPPLEMENTS TO PROTECTED HEALTH INFOR-
MATION.

(a) IN GENERAL.—Not later than 45 days after the
date on which a health care provider, health researcher,
health plan, employer, health or life insurer, school, or uni-
versity, or the agent of any such individual or entity, re-
ceives from an individual a request in writing to supple-
ment information, such entity shall—

(1) add the supplement requested to the
records;
(2) inform the individual of the supplement that has been added; and

(3) make reasonable efforts to inform any person to whom the portion of the unsupplemented information was previously disclosed, of any nontechnical supplement that has been made.

(b) REFUSAL TO SUPPLEMENT.—If an entity described in subsection (a) declines to make the supplement requested under such subsection, the entity shall inform the individual in writing of—

(1) the reasons for declining to make the supplement;

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

(3) the individual’s right to file with the entity a concise statement setting forth the requested supplement and the individual’s reasons for disagreeing with the declining entity and the individual’s right to include a copy of this refusal in his or her health record.

(c) STATEMENT OF DISAGREEMENT.—If an individual has filed a statement of disagreement under subsection (b)(3), the entity involved, 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; and

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

(d) RULES GOVERNING AGENTS.—The agent of an entity described in subsection (a) shall not be required to make supplements to protected health information, except where—

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

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

SEC. 103. NOTICE OF PRIVACY PRACTICES.

(a) PREPARATION OF WRITTEN NOTICE.—A health care provider, health plan, health oversight agency, public health authority, employer, health researcher, health or life insurer, school, or university, or the agent of any such individual or entity, shall prepare a written notice of the privacy practices of the entity that shall include—

(1) the procedures for an individual to authorize disclosures of protected health information, and to object to, modify, and revoke such authorizations;

(2) the right of an individual to inspect, copy, and supplement the protected health information;
(3) the right of an individual not to have employment or the receipt of services conditioned upon the execution by the individual of an authorization for disclosure;

(4) a description of the categories or types of employees, by general category or by general job description, who have access to or use of protected health information within the entity;

(5) a simple, concise description of any information systems used to store or transmit protected health information, including a description of any linkages made with other electronic systems or databases outside the entity;

(6) the right of the individual to request segregation of protected health information, and to restrict the use of such information by employees, agents, and contractors of an entity;

(7) the circumstances under which the information may be used or disclosed without an authorization executed by the individual; and

(8) a statement that an individual may self pay for health care in order that no identifying information be disclosed to anyone other than the health care provider unless such disclosure is related to the medical treatment or is authorized by mandatory re-
porting requirements or other similar information
collection duties as required by law.

(b) Provision and Posting of Written Notice.—

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

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

and

(B) upon the request of an individual.

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

(c) Model Notice.—The director of the Office of
Health Information Privacy, after notice and opportunity
for public comment, shall develop and disseminate model
notices of privacy practices, and model summary notices
for posting, for use under this section.
Subtitle B—Establishment of Safeguards

SEC. 111. ESTABLISHMENT OF SAFEGUARDS.

(a) In General.—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 the agent of any such individual or entity, shall establish and maintain appropriate administrative, organizational, technical, and physical safeguards and procedures to ensure the confidentiality, security, accuracy, and integrity of protected health information created, received, obtained, maintained, used, transmitted, or disposed of by such entity.

(b) Model Guidelines.—The director of the Office of Health Information Privacy, after notice and opportunity for public comment, shall develop and disseminate model guidelines for the establishment of safeguards for use under this section such as, where appropriate, individual authentication of uses of computer systems, access controls, audit trails, physical security, protection of remote access points and protection of external electronic communications, periodic security assessments, incident internal reports in sanctions, and such other systems as new technologies and problems develop. The director shall
updat and disseminate such new guidelines, as appro-
riate to take advantage of new technologies.

SEC. 112. ACCOUNTING FOR DISCLOSURES.

(a) IN GENERAL.—

(1) RECORD OF DISCLOSURE.—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 the agent of any such individual or en-
tity, shall establish and maintain, with respect to
any protected health information disclosure that is
not related to payment or treatment, a record of the
disclosure in accordance with regulations issued by
the director of the Office of Health Information Pri-

(2) AGENT.—An agent shall maintain a record
of disclosures made pursuant to subtitles B and C
of title III.

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

(c) ELECTRONIC RECORDS.—A health care provider,
health plan, health oversight agency, public health author-
ity, employer, health researcher, law enforcement official,
health or life insurer, school, or university, or the agent
of any such individual or entity, shall, to the extent practicable, maintain an electronic record, or the ability to generate such a record, concerning each attempt that is made by such an entity, or by any other person, whether authorized or unauthorized, successful or unsuccessful, to access protected health information maintained by such entity in electronic form. The record shall include the identity of the specific individual attempting to gain such access, or a way to identify that individual, and other appropriate information, and information sufficient to identify the information sought.

TITLE II—RESTRICTIONS ON USE AND DISCLOSURE
Subtitle A—General Restriction

SEC. 201. GENERAL RULE REGARDING USE AND DISCLOSURE.

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 the agent of any such individual or entity, may not disclose protected health information except as authorized under this title.
SEC. 202. AUTHORIZATIONS FOR DISCLOSURE OF PROTECTED HEALTH INFORMATION.

(a) Written Authorizations.—A health care provider, health plan, health oversight agency, public health authority, employer, health researcher, health or life insurer, school, or university, or the agent of any such individual or entity, may disclose protected health information pursuant to an authorization executed by the individual who is the subject of the information that meets the requirements of subsection (b).

(b) Requirements for Individual Authorization.—To be valid, an authorization to disclose individually identifiable health care information shall—

(1) identify the type of person (by title, general job description, or other functional description) or entity authorized to disclose protected health information;

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

(3) identify the type of person or entity (including identification made with respect to employees through use of a job description, title, or other functional description) to whom the information is to be disclosed, including individuals employed by or operating within the entity;

(4) describe the purpose of the disclosure;
(5) permit an individual to indicate that a particular person or entity listed on the authorization is not authorized to receive protected health information concerning the individual, except that a physician directly responsible for providing necessary medical care, and those directly assisting such physician, shall be permitted access to files related to providing that medical care;

(6) provide the means by which an individual may indicate that some of the individual’s protected health information should be segregated;

(7) permit an individual to indicate that protected health information, other than administrative billing information, shall not be transmitted outside the entity in a computerized, digital, optical, or other electronic format;

(8) 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; and

(9)(A) be either—

(i) in writing, dated, and signed by the individual; or
(ii) in electronic form, dated and authenti-
cated by the individual using a unique identi-
fier; and

(B) not have been revoked under paragraph (8).

(c) LIMITATION ON AUTHORIZATIONS.—

(1) IN GENERAL.—Subject to paragraphs (3)
and (4), an entity described in subsection (a) that
seeks an authorization under such subsection may
not condition the delivery of treatment or payment
for services on the receipt of an authorization.

(2) AUTHORIZATION FOR PAYMENT PUR-
POSES.—An entity described in subsection (a) that
seeks an authorization under such subsection may
not condition delivery of health care or payment for
services upon receipt of an authorization to link, ag-
gregate, match, index or associate protected health
information contained within a computerized, digital,
optical or other electronic format with other such in-
formation held by another entity.

(3) RIGHT TO REQUIRE SELF PAYMENT.—If an
individual has refused to provide an authorization of
disclosure of administrative billing information to a
person or entity and such authorization is necessary
for a health care provider to receive payment for
services delivered, the person or entity seeking the
authorization may require the individual to self-pay for the services.

(4) Authorization for treatment purposes.—If a health care provider that is seeking an authorization for disclosure of an individual’s protected health information believes that the disclosure of such information is necessary so as not to endanger the health or treatment of the individual, the health care provider may condition the provision of services upon the execution of the authorization by the individual.

(d) Model Authorizations.—The Secretary, after notice and opportunity for public comment, shall develop and disseminate model written authorizations of the type described in subsection (a) and model statements of the limitations on authorizations. Any authorization obtained on a model authorization form developed by the Secretary pursuant to the preceding sentence shall be deemed to meet the authorization requirements of this section.

(e) General Rules Applying to Authorizations for Disclosure.—

(1) Scope of disclosure.—The disclosure of protected health information under an authorization provided under this section shall be limited to the minimum amount of information necessary to ac-
complish the purpose for which the authorization
was executed.

(2) **Use of Disclosure for Purpose Only.**—A recipient of information pursuant to an
authorization under this section may use or disclose
such information solely to carry out the purpose for
which the information was authorized for release.

(3) **No General Requirement to Disclose.**—Nothing in this section permitting the dis-
closure of protected health information shall be con-
strued to require such disclosure.

(4) **Identification of Disclosed Information as Protected Health Information.**—Pro-
tected health information disclosed pursuant to an
authorization under this section shall be clearly iden-
tified as protected health information that is subject
to this Act.

(f) **Segregation of Files.**—An entity described in
subsection (a) shall comply with the request of an individ-
ual who is the subject of protected health information to—

(1) segregate any type or amount of protected
health information, other than administrative billing
information, held by the entity;

(2) limit the use or disclosure of the segregated
health information within the entity to those persons
specifically designated by the subject of the pro-
tected health information; and

(3) maintain such information outside any
networked computerized, digital, optical or other
electronic system.

(g) Revocation of Authorization.—

(1) In general.—An individual may 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 pay-
ment for health care that has been provided to the
individual.

(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-re-
newal 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 person-
ally identifiable health information—

(A) if the disclosure was made based on a
good faith reliance on the individual’s author-
ization at the time disclosure was made;
(B) in a case in which the authorization is revoked, if the disclosing entity 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, if authorized under section 211.

(h) **RECORD OF INDIVIDUAL’S AUTHORIZATIONS AND REVOCATIONS.**—Each person collecting or storing personally identifiable health information shall maintain a record for a period of 7 years of each authorization of an individual and any revocation thereof, and such record shall become part of the personally identifiable health information concerning such individual.

(i) **NO WAIVER.**—Except as provided for in this Act, an authorization to disclose personally identifiable health information by an individual 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.

(j) **RULE OF CONSTRUCTION.**—Except as provided in subsection (a), nothing in this section shall be construed to prevent the electronic or computerized exchange of administrative billing information for the purpose of a claims payment.

(k) **DEFINITION.**—For purposes of this section—
the term “segregate” means to place a designated subset of protected health information in a location or computer file that is separate from the location or computer file used to store general protected health information and where access to or use of any information so segregated may be effectively limited to those individuals who are authorized to access or use such information; and

(2) the terms “signed” refers to both signatures in ink and electronic signatures, and “written” refers to both paper and computerized formats.

Subtitle B—Limited Circumstances Providing for Disclosure Without Authorization

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 practitioner, health care facility, law enforcement authority, or emergency medical personnel to protect the health or safety of such subject.

(b) Harm to Others.—In the event of a threat of harm to an individual other than the subject of protected
health information, any person may disclose protected
health information about such subject where—

(1) there is an identifiable threat of serious in-
jury or death to an identifiable individual or group
of individuals;

(2) the subject of the protected health informa-
tion 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.

(c) LIMITATIONS.—

(1) Scope of disclosure.—Every disclosure
of protected health information under this section
shall be limited to the minimum amount of informa-
tion necessary to achieve the purposes of this sec-
tion.

(2) Use or disclosure for purpose
only.—A recipient of information pursuant to this
section may use or disclose such information solely
to carry out the purposes of this section.

(3) Identification of disclosed informa-
tion as protected health information.—Pro-
tected health information disclosed under this sec-
tion must be clearly identified as protected health in-
formation that is subject to this Act.
SEC. 212. PUBLIC HEALTH.

(a) GENERAL RULE.—A health care provider, health plan, public health authority, health researcher, employer, law enforcement official, health or life insurer, school or university, or the agent of any such individual or entity, may disclose protected health information concerning an individual to a public health authority where—

(1) there is a specific nexus between the individual’s identity and a threat of a specific disease, death, or injury to any individual or to the public health; and

(2) the individual’s identity would allow such public health authority to prevent or significantly reduce the possibility of injury or death to any individual or the public health, such as the creation and use of disease registries established under Federal or State law.

(b) EXCEPTION.—An entity described in subsection (a) shall not be liable for the disclosure of protected health information—

(1) to a public health authority based upon a good faith belief and credible representation made by such authority that such information was required to protect an individual or the public health from a threat of a specific disease, injury, or death; or
(2) if such disclosure is made pursuant to Federal or state laws which are designed to protect the public health or safety.

SEC. 213. PROTECTION AND ADVOCACY AGENCIES.

(a) General Rule.—Any person who creates or receives protected health information under this title may disclose protected health information to an agency charged by law to protect the health and safety of individuals when such agency 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 or neglect by an entity providing health or social services to such individual.

(b) Limitations.—

(1) Scope of disclosure.—Every disclosure of protected health information under this section shall be limited to the minimum amount of information necessary to achieve the purposes of this section.

(2) Use or disclosure for purpose only.—A recipient of information pursuant to this section may use or disclose such information solely to achieve the purposes of this section.

(3) Identification of disclosed information as protected health information.—Pro-
tected health information disclosed under this sec-
ction must be clearly identified as protected health in-
formation that is subject to this Act.

SEC. 214. OVERSIGHT.

(a) General Rule.—A health care provider, health
plan, public health authority, health researcher, employer,
law enforcement official, health or life insurer, school or
university, or the agent of any such individual or entity,
may disclose protected health information concerning an
individual to a health oversight agency to enable the agen-
cy to perform a health oversight function authorized by
law only if the agency—

(1) does not record the name, social security
number, or other identifying information of the indi-
vidual from patient or client files;

(2) identifies the individual in all workpapers
and electronic records by either relying upon a unit
record number contained in the file or by using an-
other formula to scramble or otherwise safeguard
the identifying information; and

(3) does not remove protected health informa-
tion from the premises, custody or control of such
entity.

(b) Nonidentifiable Information.—An entity de-
scribed in subsection (a) may disclose health information
concerning an individual to a health oversight agency to
perform a health oversight function authorized by law
when any information that could reasonably be expected
to identify the individual has been removed or concealed.

(c) Prohibition in Use in Action Against Individuals.—Protected health information about an individ-
ual 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.

(d) Authorization by a Supervisor.—For pur-
poses of this section, the individual with authority to au-
thorize the oversight function involved shall provide to the
entity described in subsections (a) or (b) a statement that
the protected health information is being sought for a le-
gally authorized oversight function.

(e) Limitations.—

(1) Scope of Disclosure.—Every disclosure
of protected health information under this section
shall be limited to the minimum amount of informa-
tion necessary to achieve the purposes of this sec-
tion.

(2) Use of Disclosure for Purpose
only.—A recipient of information pursuant to this
section may use or disclose such information solely to achieve the purposes of this section.

(3) **NO GENERAL REQUIREMENT TO DISCLOSE.**—Nothing in this section permitting the disclosure of protected health information shall be construed to require such disclosure.

(4) **IDENTIFICATION OF DISCLOSED INFORMATION AS PROTECTED HEALTH INFORMATION.**—Protected health information disclosed under this section must be clearly identified as protected health information that is subject to this Act.

**SEC. 215. DISCLOSURE FOR LAW ENFORCEMENT PURPOSES.**

(a) **LAW ENFORCEMENT ACCESS TO PROTECTED HEALTH INFORMATION.**—A health care provider, health researcher, health plan, health oversight agency, employer, health or life insurer, school, university, or the agent of any such individual or entity, or person who receives protected health information pursuant to section 211, may disclose protected health information to a law enforcement authority only if the disclosure is made pursuant to a court order issued by a court of competent jurisdiction in accordance with subsections (b) and (e) or otherwise ordered by a Court of competent jurisdiction.
(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 law enforcement authority involved submits a written application upon oath or affirmation and demonstrates by clear and convincing evidence that—

(1) the protected health information sought is necessary to a legitimate law enforcement inquiry into a particular violation of criminal law being conducted by the authority;

(2) the investigative or evidentiary needs of the law enforcement authority cannot be satisfied by nonidentifiable health information or by any other information; and

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

(c) 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 under this section unless notice of the application for the order has been served on the individual who is the subject of the information in-
volved 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 individual if the court finds, by clear and convincing evidence, that notice would be impractical because—

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

(B) notice would risk destruction or unavailability of the evidence.

(d) CONDITIONS.—Upon the granting of an order for disclosure of protected health information under this section, the court shall impose appropriate safeguards to ensure the confidentiality of such information and to protect against unauthorized or improper use or disclosure.

(e) LIMITATION ON USE AND DISCLOSURE FOR OTHER LAW ENFORCEMENT INQUIRIES.—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, any administrative, civil, or criminal action or investigation directed against the individual, unless the action or investigation arises out of, or is directly related to, the law enforcement inquiry for which the information was obtained.
(f) **DESTRUCTION OR RETURN OF INFORMATION.**—
When the matter or need for which protected health information was disclosed to a law enforcement agency or grand jury has concluded, including any derivative matters arising from such matter or need, the law enforcement agency or grand jury shall either destroy the protected health information, or return it to the person from whom it was obtained.

(g) **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.

(h) **LIMITATIONS.**—

(1) **SCOPE OF DISCLOSURE.**—Every disclosure of protected health information under this section shall be limited to the minimum amount of information necessary to fulfill the purposes of this section.

(2) **USE OR DISCLOSURE FOR PURPOSE ONLY.**—A recipient of information pursuant to this section may use or disclose such information solely to fulfill the purposes of this section.

(3) **IDENTIFICATION OF DISCLOSED INFORMATION AS PROTECTED HEALTH INFORMATION.**—Pro-
tected health information disclosed under this sec-

section must be clearly identified as protected health in-

formation that is subject to this Act.

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

Subtitle C—Special Rules

Governing Disclosure

SEC. 221. NEXT OF KIN AND DIRECTORY INFORMATION.

(a) NEXT OF KIN.—A health care provider, or a per-

son who receives protected health information under sec-

tion 211, may not disclose protected health information
regarding an individual to the individual’s next of kin, or
to another person whom the individual has identified, un-
less at the time of the treatment of the individual—

(1) the individual who is the subject of the in-

formation—

(A) has been notified of the individual’s

right to object to such disclosure and the indi-

vidual has not objected to the disclosure; or

(B) is in a physical or mental condition

such that the individual is not capable of object-

ing, and there are no prior indications that the

individual would object; and
(2) the information disclosed relates to health care currently being provided to that individual.

(b) Directory Information.—

(1) Disclosure.—

(A) In general.—Except as provided in paragraph (2), an entity described in subsection (a) may not disclose the information described in subparagraph (B) to any person unless, at the time of the admission of the individual who is the subject of the information to a facility, the individual—

(i) has been notified of the individual’s right to object and the individual 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 on premises controlled by a provider.

(2) Exception.—

(A) Location.—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.

(B) Directory or Next of Kin Information.—A disclosure may not be made under this section if the health care provider involved 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.

(c) Identification of Deceased Individual.— An entity described in subsection (a) may disclose protected health information if such disclosure is necessary to assist in the identification of a deceased individual.

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

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

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

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

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

(B) 14 through 17 years of age, the rights of inspection and supplementation, and the right to authorize use and disclosure of protected health information of the individual shall be exercised by the individual, or by the parent or legal guardian of the individual.
(c) **General Rules Applying to Disclosures of Protected Health Information With Respect to Next of Kin and Directory Information.**—

(1) **Scope of disclosure.**—Every disclosure of protected health information under this section shall be limited to the minimum amount of information necessary to achieve the purposes of this section.

(2) **No general requirement to disclose.**—Nothing in this section permitting the disclosure of protected health information shall be construed to require such disclosure.

**SEC. 222. HEALTH RESEARCH.**

(a) **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 research conducted by all research facilities using personally identifiable health information. The Secretary shall promulgate regulations to implement this subsection through notice and comment rulemaking.

(b) **Evaluation.**—Not later than 1 year 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 personally identifiable data can be used for medical 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 under what circumstances informed consent is being waived and the extent to which the privacy of individuals is taken into account as a factor before allowing waivers;

(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 waiving informed consent; and

(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.

(d) COMPLIANCE WITH DEADLINE.—Notwithstanding any other provision of law, if the Secretary does not submit the recommendations to Congress by the date described in subsection (b), the authority of the Secretary
to permit the conduct of medical research using personally identifiable data without written informed consent shall be terminated.

(e) 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.

(f) 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 notice and comment rulemaking and shall advise Congress of such proposal.

(g) TERMINATION OF INCONSISTENT AUTHORITY.—Notwithstanding any other provision of law, if the Secretary determines that prior written informed consent is appropriate for some or all research using personally identifiable health information, the authority of the Secretary to promulgate regulations inconsistent with that determination shall be terminated 6 months after the date on which such determination is made pursuant to this Act.

(h) OTHER REQUIREMENTS.—
(1) Obligations of the recipient.—A person who receives protected health information pursuant to this section—

(A) 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—

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

(ii) there is an adequate plan to protect the identifiers from disclosure consistent with this section; and

(2) Periodic review and technical assistance.—

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

(B) Technical assistance.—The Secretary may provide technical assistance to institutional review boards described in this subsection.
(C) MONITORING.—The Secretary shall periodically monitor institutional review boards described in this subsection.

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

(i) LIMITATION.—Nothing in this section shall be construed to permit personally identifiable 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.

SEC. 223. JUDICIAL AND ADMINISTRATIVE PURPOSES.

(a) IN GENERAL.—A health care provider, health plan, health oversight agency, employer, insurer, health or life insurer, school or university, or the agent of any such individual or entity, or person who receives protected health information under section 211, may disclose protected health information—

(1) pursuant to the standards and procedures established in the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure, or comparable rules of other courts or administrative agencies, in connection with litigation or proceedings to
which the individual who is the subject of the infor-
mation 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 pursuant
to a law requiring the reporting of specific medical
information to law enforcement authorities.

(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 affirmation and dem-
onstrates 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 or criminal proceeding;

(2) the adjudicative need cannot be satisfied by
nonidentifiable health information or by any other
information; and
(3) the need for the information outweighs the
privacy interest of the individual to whom the infor-
mation pertains.

(c) 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 is-
sued 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 op-
pose 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-
vidual 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.—

(1) IN GENERAL.—A person seeking protected
health information pursuant to paragraph (1) of
subsection (a)—
(A) shall notify the individual or the individual’s attorney of the request for the information;

(B) shall provide the health care provider, health plan, health oversight agency, employer, insurer, health or life insurer, school or university, or agent, or person involved with a signed document attesting—

(i) that the individual has placed his or her physical or mental condition at issue in litigation or proceedings in which the individual is a party; and

(ii) the date on which the individual or the individual’s attorney was notified under subparagraph (A); and

(C) 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, or agent, or person until the termination of the 10-day period beginning on the date notice was given under subparagraph (A).

(2) Disclosure for purpose only.—A person who receives protected health information pursuant to subsection (a) may disclose the information
only to accomplish the purpose for which the pro-
tected health information was obtained.

(e) LIMITATIONS.—

(1) Scope of disclosure.—Every disclosure
of protected health information under this section
shall be limited to the minimum amount of informa-
tion necessary to achieve the purposes of this sec-
tion.

(2) No general requirement to dis-
close.—Nothing in this section permitting the dis-
closure of protected health information shall be con-
strued to require such disclosure.

(3) Identification of disclosed informa-
tion as protected health information.—Pro-
tected health information disclosed under this sec-
tion must be clearly identified as protected health in-
formation that is subject to this Act.

SEC. 224. 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 the individual being a minor), or by
an instrument recognized under law, to act as an agent,
attorney, proxy, or other legal representative of a pro-
tected individual, may, to the extent so authorized, exer-
(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 authorize disclosure under this Act may be exercised and discharged in the best interest of the individual by—

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

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

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

(d) Application to Deceased Individuals.—The provisions of this Act shall continue to apply to protected health information concerning a deceased individual for a period of 2 years following the death of that individual.

(e) 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 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 for a period of 2 years following the death of that individual. If no such designee has been authorized, the rights of the deceased individual may be exercised as provided for in subsection (c).

SEC. 325. PROHIBITION AGAINST RETALIATION.

A health care provider, health researcher, health plan, health oversight agency, employer, health or life insurer, school or university, or the agent of any such indi-
individual or entity, or person who receives protected health information under section 211 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 assisted a person in the exercise of a right under this Act.

TITLE III—OFFICE OF HEALTH INFORMATION PRIVACY OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES

Subtitle A—Establishment

SEC. 301. ESTABLISHMENT.

(a) IN GENERAL.—There is established within the Department of Health and Human Services an office to be known as the Office of Health Information Privacy. The Office shall be headed by a director, who shall be appointed by the Secretary.

(b) DUTIES.—The Director of the Office of Health Information Privacy 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 in the implementation of this Act;

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

(5) 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

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

(c) REPORT ON COMPLIANCE.—Not later than January 1, 1999, and every January 1 thereafter, the Director of the Office of Health Information Privacy 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.

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.

§ 2801. Wrongful disclosure of protected health information

(a) OFFENSE.—The penalties described in subsection (b) shall apply to a person that knowingly and intentionally—

“(1) obtains protected health information relating to an individual in violation of title II of the Medical Information Privacy and Security Act; or

“(2) discloses protected health information to another person in violation of title II of the Medical Information Privacy and Security Act.

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

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

“(2) if the offense is committed under false pretenses, be fined not more than $250,000, imprisoned not more than 5 years, or any combination of such penalties;

“(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, excluded from par-
ticipation in any Federally funded health care pro-
grams, or any combination 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-
f erent 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 follow-
ing new item:

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

SEC. 312. DEBARMENT FOR CRIMES.

(a) Purpose.—The purpose of this section is to pro-
mote the prevention and deterrence of instances of inten-
tional criminal actions which violate criminal laws which
are designed to protect the privacy of protected health in-
formation in a manner consistent 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 regu-
lations and establish procedures to permit the debarment
of health care providers, health researchers, health or life
insurers, or schools or universities from receiving benefits
under any Federal health programs if the managers or
officers of such entities are found guilty of violating sec-
tion 2801 of title 18, United States Code, have civil pen-
alties imposed against such officers or managers under
section 321 in connection with the illegal disclosure of pro-
tected health information, or are found guilty of making
a false statement or obstructing justice related to attempt-
ing to conceal 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 debar-
ment imposed under this section to take into account the
medical needs of patients.

(c) Consultation.—Before 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 individuals and entities, to gain additional in-
formation regarding the debarment of entities under sub-
section (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) VIOLATION.—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, or the agent of any such individual or entity, who the Office of Health Information Privacy, in consultation with the Attorney General, determines has substantially and materially failed to com-
ply 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 $5000 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 the Office finds that such violations have occurred with such frequency as to constitute a general business practice, to a civil penalty of not more than $100,000.

(b) PROCEDURES FOR IMPOSITION OF PENALTIES.—Section 1128A of the Social Security Act, other than subsections (a) and (b) and the second sentence of subsection (f) of that section, shall apply to the imposition of a civil, monetary, or exclusionary penalty under this section in the same manner as such provisions apply with respect to the imposition of a penalty under section 1128A of such Act.

SEC. 322. PROCEDURES FOR IMPOSITION OF PENALTIES.

(a) INITIATION OF PROCEEDINGS.—

(1) IN GENERAL.—The director of the Office of Health Information Privacy, in consultation with the
Attorney General, may initiate a proceeding to determine whether to impose a civil money penalty under section 321. The director 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 director may initiate an action under this section by serving notice of the action in any manner authorized by Rule 4 of the Federal Rules of Civil Procedure.

(2) Notice and Opportunity for Hearing.—The director of the Office of Health Information Privacy shall not make a determination adverse to any person under paragraph (1) until the person has been given written notice and an opportunity for the determination to be made on the record after a hearing at which the person is entitled to be represented by counsel, to present witnesses, and to cross-examine witnesses against the person.

(3) Estoppel.—In a proceeding under paragraph (1) that—

(A) is against a person who has been convicted (whether upon a verdict after trial or upon a plea of guilty or nolo contendere) of a
crime under section 2801 of title 18, United States Code; and

(B) involves the same conduct as in the criminal action;

the person is estopped from denying the essential elements of the criminal offense.

(4) SANCTIONS FOR FAILURE TO COMPLY.—
The official conducting a hearing under this section may sanction a person, including any party or attorney, for failing to comply with an order or procedure, failing to defend an action, or other misconduct as would interfere with the speedy, orderly, or fair conduct of the hearing. Such sanction shall reasonably relate to the severity and nature of the failure or misconduct. Such sanction may include—

(A) in the case of refusal to provide or permit discovery, drawing negative factual inferences or treating such refusal as an admission by deeming the matter, or certain facts, to be established;

(B) prohibiting a party from introducing certain evidence or otherwise supporting a particular claim or defense;

(C) striking pleadings, in whole or in part;

(D) staying the proceedings;
(E) dismissal of the action;

(F) entering a default judgment;

(G) ordering the party or attorney to pay attorneys’ fees and other costs caused by the failure or misconduct; and

(H) refusing to consider any motion or other action which is not filed in a timely manner.

(b) Scope of Penalty.—In determining the amount or scope of any penalty imposed pursuant to section 321, the director of the Office of Health Information Privacy 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 offenses, and financial condition of the person presenting the claims; and

(3) such other matters as justice may require.

(c) Review of Determination.—

(1) In general.—Any person adversely affected by a determination of the director of the Office of Health Information Privacy under this section may obtain a review of such determination in the United States Court of Appeals for the circuit in which the person resides, or in which the claim
was presented, by filing in such court (within 60
days following the date the person is notified of the
determination of the director) a written petition re-
questing that the determination be modified or set
aside.

(2) FILING OF RECORD.—A copy of the petition
filed under paragraph (1) shall be forthwith trans-
mitted by the clerk of the court to the director of
the Office of Health Information Privacy, and there-
upon the director shall file in the Court the record
in the proceeding as provided in section 2112 of title
28, United States Code. Upon such filing, the court
shall have jurisdiction of the proceeding and of the
question determined therein, and shall have the
power to make and enter upon the pleadings, testi-
mony, and proceedings set forth in such record a de-
cree affirming, modifying, remanding for further
consideration, or setting aside, in whole or in part,
the determination of the director and enforcing the
same to the extent that such order is affirmed or
modified.

(3) CONSIDERATION OF OBJECTIONS.—No ob-
jection that has not been raised before the director
of the Office of Health Information Privacy with re-
spect to a determination described in paragraph (1)
shall be considered by the court, unless the failure
or neglect to raise such objection shall be excused
because of extraordinary circumstances.

(4) FINDINGS.—The findings of the director of
the Office of Health Information Privacy with re-
spect to questions of fact in an action under this
subsection, if supported by substantial evidence on
the record considered as a whole, shall be conclusive.
If any party shall apply to the court for leave to ad-
duce additional evidence and shall show to the satis-
faction of the court that such additional evidence is
material and that there were reasonable grounds for
the failure to adduce such evidence in the hearing
before the director, the court may order such addi-
tional evidence to be taken before the director and
to be made a part of the record. The director may
modify findings as to the facts, or make new find-
ings, by reason of additional evidence so taken and
filed, and shall file with the court such modified or
new findings, and such findings with respect to
questions of fact, if supported by substantial evi-
dence on the record considered as a whole, and the
recommendations of the director, if any, for the
modification or setting aside of the original order,
shall be conclusive.
(5) **EXCLUSIVE JURISDICTION.**—Upon the filing of the record with the court under paragraph (2), the jurisdiction of the court shall be exclusive and its judgment and decree shall be final, except that the same shall be subject to review by the Supreme Court of the United States, as provided for in section 1254 of title 28, United States Code.

(d) **RECOVERY OF PENALTIES.**—

(1) **IN GENERAL.**—Civil money penalties imposed under this chapter may be compromised by the director of the Office of Health Information Privacy and 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 resides, as determined by the director. Amounts recovered under this section shall be paid to the director and deposited as miscellaneous receipts of the Treasury of the United States.

(2) **DEDUCTION FROM AMOUNTS OWING.**—The amount of any penalty, when finally determined under this section, or the amount agreed upon in compromise under paragraph (1), 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.

(e) Determination Final.—A determination by the director of the Office of Health Information Privacy to impose a penalty under section 321 shall be final upon the expiration of the 60-day period referred to in subsection (c)(1). Matters that were raised or that could have been raised in a hearing before the director or in an appeal pursuant to subsection (e) may not be raised as a defense to a civil action by the United States to collect a penalty under section 321.

(f) Subpoena Authority.—

(1) In General.—For the purpose of any hearing, investigation, or other proceeding authorized or directed under this section, or relative to any other matter within the jurisdiction of the Attorney General hereunder, the Attorney General, acting through the director of the Office of Health Information Privacy shall have the power to issue subpoenas requiring the attendance and testimony of witnesses and the production of any evidence that relates to any matter under investigation or in question before the director. Such attendance of witnesses and production of evidence at the designated place of such hearing, investigation, or other pro-
ceeding may be required from any place in the Unit-
ed States or in any Territory or possession thereof.

(2) SERVICE.—Subpoenas of the director under
paragraph (1) shall be served by anyone authorized
by the director by delivering a copy thereof to the
individual named therein.

(3) PROOF OF SERVICE.—A verified return by
the individual serving the subpoena under this sub-
section setting forth the manner of service shall be
proof of service.

(4) FEES.—Witnesses subpoenaed under this
subsection shall be paid the same fees and mileage
as are paid witnesses in the district court of the
United States.

(5) REFUSAL TO OBEY.—In case of contumacy
by, or refusal to obey a subpoena duly served upon,
any person, any district court of the United States
for the judicial district in which such person charged
with contumacy or refusal to obey is found or re-
sides or transacts business, upon application by the
director of the Office of Health Information Privacy,
shall have jurisdiction to issue an order requiring
such person to appear and give testimony, or to ap-
pear and produce evidence, or both. Any failure to
obey such order of the court may be punished by the
court as contempt thereof.

(g) INJUNCTIVE RELIEF.—Whenever the director of
the Office of Health Information Privacy 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
director 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, encumber-
ing, 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.

(h) AGENCY.—A principal is liable 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 liq-
uidated 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.

**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 pri-
vacy of, and access to, their health information that are
greater than those provided for in this Act.

(b) Privileges.—Nothing in this Act shall be con-
strued to preempt or modify any provisions of State statu-
tory 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 person
in a court of the United States. Authorizations pursuant
to section 202 shall not be construed as a waiver of any
such privilege.

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

(1) provides for the reporting of vital statistics
such as birth or death information;
(2) requires the reporting of abuse or neglect
information about any individual;
(3) regulates the disclosure or reporting of in-
formation concerning an individual’s mental health
or communicable disease status otherwise permis-
sible under this Act; 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 thereof the following: “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 person who receives protected health information under section 211 of the Medical 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(19) 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 fol-
(e) CONSTITUTION.—Nothing in this Act shall be construed to alter, diminish, or otherwise weaken existing legal standards under the Constitution regarding the confidentiality of protected health information.

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 promulgation of the regulations required under subsection (b) but in no event later than the date that is 30 months after the date of enactment of this Act or 6 months after the promulgation of such regulations, 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 director of the Office of Health Information Privacy shall promulgate regulations implementing this Act.