number of well-trained mental health service professionals (including those based in schools) providing clinical mental health care to children and adolescents, and for other purposes.

S. 1669

At the request of Ms. STABENOW, the name of the Senator from California (Mrs. BOXER) was added as a cosponsor of S. 1669, a bill to amend titles XIX and XXI of the Social Security Act to ensure payment under Medicaid and the State Children's Health Insurance Program (SCHIP) for covered items and services furnished by school-based health clinics.

S. 1743

At the request of Mr. HATCH, the name of the Senator from Oregon (Mr. SMITH) was added as a cosponsor of S. 1743, a bill to amend the Internal Revenue Code of 1986 to repeal the dollar limitation on contributions to funeral trusts.

S. 1755

At the request of Mr. CASEY, the name of the Senator from Massachusetts (Mr. KERRY) was added as a cosponsor of S. 1755, a bill to amend the Richard B. Russell National School Lunch Act to make permanent the summer food service pilot project for rural areas of Pennsylvania and apply the program to rural areas of every State.

S. 1793

At the request of Mrs. CLINTON, the name of the Senator from Oregon (Mr. SMITH) was added as a cosponsor of S. 1793, a bill to amend the Internal Revenue Code of 1986 to provide a tax credit for property owners who remove lead-based paint hazards.

S. 1800

At the request of Mrs. CLINTON, the names of the Senator from Massachusetts (Mr. KERRY), the Senator from California (Mrs. FEINSTEIN) and the Senator from New Jersey (Mr. MENENDEZ) were added as cosponsors of S. 1800, a bill to amend title 10, United States Code, to require emergency contraception to be available at all military health care treatment facilities.

S. RES. 178

At the request of Mr. BINGAMAN, the names of the Senator from Illinois (Mr. DURBIN) and the Senator from California (Mrs. FEINSTEIN) were added as cosponsors of S. Res. 178, a resolution expressing the sympathy of the Senate to the families of women and girls murdered in Guatemala, and encouraging the United States to work with Guatemala to bring an end to these crimes.

S. RES. 221

At the request of Mr. CRAPO, the name of the Senator from Mississippi (Mr. COCHRAN) was added as a cosponsor of S. Res. 221, a resolution supporting National Peripheral Arterial Disease Awareness Month and efforts to educate people about peripheral arterial disease.

AMENDMENT NO. 2000

At the request of Mr. NELSON of Florida, the name of the Senator from Louisiana (Ms. LANDRIEU) was added as a cosponsor of amendment No. 2000 intended to be proposed to H.R. 1585, to authorize appropriations for fiscal year 2008 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 2056

At the request of Mr. HARKIN, the name of the Senator from Oregon (Mr. WYDEN) was added as a cosponsor of amendment No. 2056 intended to be proposed to H.R. 1585, to authorize appropriations for fiscal year 2008 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 2074

At the request of Mrs. LINCOLN, the name of the Senator from Colorado (Mr. SALAZAR) was added as a cosponsor of amendment No. 2074 intended to be proposed to H.R. 1585, to authorize appropriations for fiscal year 2008 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 2127

At the request of Mr. WEBB, the name of the Senator from Iowa (Mr. HARKIN) was added as a cosponsor of amendment No. 2127 intended to be proposed to H.R. 1585, to authorize appropriations for fiscal year 2008 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 2206

At the request of Mr. WEBB, the names of the Senator from Michigan (Mr. LEVIN), the Senator from Illinois (Mr. DURBIN), the Senator from California (Mrs. FEINSTEIN), the Senator from Massachusetts (Mr. KERRY), the Senator from Delaware (Mr. CARPER), the Senator from South Dakota (Mr. JOHNSON), the Senator from California (Mrs. BOXER) and the Senator from Illinois (Mr. OBAMA) were added as cosponsors of amendment No. 2206 intended to be proposed to H.R. 1585, to authorize appropriations for fiscal year 2008 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 2221

At the request of Mr. KERRY, the name of the Senator from Maine (Ms. SNOWE) was added as a cosponsor of amendment No. 2221 intended to be proposed to H.R. 1585, to authorize appropriations for fiscal year 2008 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 2291

At the request of Ms. CANTWELL, the name of the Senator from Oregon (Mr. WYDEN) was added as a cosponsor of amendment No. 2291 intended to be proposed to H.R. 1585, to authorize appropriations for fiscal year 2008 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 2310

At the request of Mr. SALAZAR, the name of the Senator from Maryland (Mr. CARDIN) was added as a cosponsor of amendment No. 2310 intended to be proposed to H.R. 1585, to authorize appropriations for fiscal year 2008 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. OBAMA (for himself, Mr. SCHUMER, and Mrs. CLINTON):

S. 1811. A bill to amend the Toxic Substances Control Act to assess and reduce the levels of lead found in child-occupied facilities in the United States, and for other purposes; to the Committee on Environmental and Public Works.

Mr. OBAMA. Mr. President, I rise today to reintroduce the Lead Poisoning Reduction Act.

Two weeks ago, the Washington Post featured an article on lead research by the economist Rick Nevin. Mr. Nevin's work demonstrates a strong link between lead exposure and criminal activity in our country. Specifically, he found that national spikes in rates of children with lead poisoning were significantly correlated with spikes in criminal activity two decades later. Notably, this finding was not unique to the U.S., he found a similar association in 9 other countries, despite differences in economics, demographics, and values. Although many readers, myself included, were surprised by Nevin's findings, the scientific community was not, having known for many years that lead poisoning leads to irrevocable, toxic effects on brain development of young children. These effects lead to changes such as impulsivity and impaired cognition, which appear to contribute to criminal behavior in later years.

Mr. Nevin's work underscores the critical importance of eliminating lead poisoning in children, which is completely preventable and has tragic consequences. In the U.S., over 300,000 children have blood lead levels of 10

micrograms or higher, the level traditionally considered to indicate ''lead poisoning''. Yet, even this level is now considered unsafe as newer research has indicated that lead-related damage starts at much lower levels. We must remain vigilant in tackling all sources of lead exposure, to save future generations of children from harm, and the Lead Poisoning Reduction Act will help to do just that.

The major source of lead exposure among U.S. children is lead-based paint and lead-contaminated dust found in deteriorating buildings. The Lead Poisoning Reduction Act will provide $42.6 million in grants to communities that wish to develop and implement lead amelioration programs for their childcare facilities. It directs EPA to promulgate regulations within 18 months that require new child-occupied facilities to be certified lead-safe before opening for business. Additionally, EPA would also promulgate regulations within 5 years of enactment to require that all non-home-based childcare facilities be lead-safe. Further, my bill requires EPA to conduct a study of State, tribal and local programs designed to protect children from lead exposure in child-occupied facilities; to establish baseline studies, based on the results of this study; and to create a model program, that can be adapted for use by State, tribal and community officials, for testing, abatement, and communication of risks of lead to children and parents.

Reducing lead hazards in our communities, especially in child-occupied facilities, is critical, with impact reaching beyond individual children in preschools in any given city, to our society as a whole. It is the right thing to do, and the smart thing to do, and it should have been done years ago.

I call on my colleagues to support the Lead Protection Reduction Act, which will help to ensure that every child has access to safe, lead-free childcare facilities in this Nation.

By Mrs. CLINTON (for herself, Mr. KERRY, Mr. AKAKA, and Mr. BAYH):

S. 1812. A bill to amend the Elementary and Secondary Education Act of 1965 to strengthen mentoring programs, and for other purposes; to the Committee on Health, Education, Labor, and Pensions.

Mrs. CLINTON. Mr. President, research indicates a caring adult can make a difference in a child's future. Today, I am pleased to introduce legislation that will expand the mentoring programs found in the No Child Left Behind Act. If adopted, the Mentoring America's Children Act of 2007 would help close America's ''mentoring gap'' and match more at-risk students with high-quality mentors. I thank my colleagues, Senators KERRY, AKAKA, and BAYH, for joining me on this important legislation.

Mentoring programs are a cost-effective way to expand a young person's ability for success. Studies have shown young people with mentors perform better in school and are more likely to graduate and go on to higher education. Mentors also play a role in improving the social and emotional well-being and reducing the negative behaviors of the children they mentor.

Despite the positive effects of having a mentor, nearly 15 million young adults are still in need of mentoring. These young people encompass America's ''mentoring gap.'' That is why I have joined with my colleagues to introduce the Mentoring America's Children Act of 2007.

This legislation broadens the reach of mentoring to include specific populations of young people who could particularly benefit from a mentor's involvement, including children in foster care and kids in communities with a high rate of youth suicides. It also provides much needed training and technical assistance to grantees, tracks youth outcomes, strengthens research on the effects of mentoring, and improves the sustainability of grant recipients. Finally, this bill allows students to gain professional skills while working with mentors by establishing internship programs during the school year.

Mentoring plays a key role in improving the learning environment for a young person, as mentored youth have better attendance and are more connected to their school, schoolwork, and teachers. Mentors serve as role models, advisors, and advocates for the children they mentor. We must work together to match even more high-quality mentors with our neediest children.

This legislation is supported by MENTOR/National Mentoring Partnership, Big Brothers Big Sisters of America and the National Collaboration for Youth. I ask my colleagues to join me in approving this legislation.

Mr. KERRY. Mr. President, our Nation's children are our greatest resource. They represent the future of this country and we should do everything we can to foster their growth and ensure they lead happy and productive lives. That is why I am proud to cosponsor the Mentoring America's Children Act of 2007 which was introduced today by Senator CLINTON. This important legislation highlights the significant impact mentoring can have on a child.

Research has shown time and time again that mentoring is an important component to a child's development. Often these children come from broken homes or communities affected by violence. The relationship formed between a mentor and a child helps support their studies in school, their relationships with their families at home, and gives them the confidence they need to withstand the pressures they are faced with. Our children are confronted with much more than some of us even realize. By providing a mentor, parents and teachers have another line of defense in allowing our children to grow up in a safe nurturing environment.

The consequences of letting young people grow up without a support system are dire. In 2006 America's law enforcement officers arrested approximately 250 teens an hour, and it's estimated that 900,000 of our children are victims of abuse and neglect. Studies show that most teens that use alcohol, cigarettes and marijuana do so before they are 14. This is unacceptable. We must do more to foster these children so they stay in school, keep clean and out of trouble.

Mentoring can help improve the social and mental well being of a child so they can deal with the myriad of challenges they face. Massachusetts has many notable mentoring programs that have affected thousands of children's lives. Strong Women, Strong Girls is a program started by a Harvard graduate that matches local university women with girls in targeted communities to help create another generation of strong women through mentoring. The Boys and Girls Club has a long and storied history in my State as does the Big Brother Big Sister program. A study of Brother Big Sister showed that children that benefited from their program were 46 percent less likely to use drugs, 52 percent less likely to skip school and have fewer conflicts with their families.

The Mentoring America's Children Act would help these programs and others like them across the country. It builds on the mentoring programs already put in place in the No Child Left Behind Act by ensuring that they are as effective as possible. The bill provides for additional training and technical resources as well as studies the efficacy of these various programs. More importantly, it widens the net of children that can be helped by mentors by focusing on children in the foster care system and those that live in communities with high suicide rates. We should be focusing our energies on helping the children most in need and providing them with mentors that can enrich their lives and help them succeed.

By Mr. LEAHY (for himself and Mr. KENNEDY):

S. 1814. 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; to the Committee on Health, Education, Labor, and Pensions.

Mr. LEAHY. Mr. President, today I am pleased to join Senator KENNEDY, the distinguished Chairman of the Committee on Health, Education, Labor Pensions, in introducing the Health Information Privacy and Security Act of 2007, HIPSA. This comprehensive health privacy bill will ensure the right to privacy with respect

to health information for millions of Americans.

In America today, if you have a health record, you have a health privacy problem. The explosion of electronic health records, digital databases and the Internet is fueling a growing supply and demand for Americans' health information. The ability to easily access this information electronically, often by the click of a mouse, or a few key strokes on a computer, can be very useful in providing more cost-effective health care. But, the use of advancing technologies to access and share health information can also lead to a loss of personal privacy.

In the Information Age, the traditional right and expectation of confidentiality between patient and doctor is at great risk. Without adequate safeguards to protect health privacy, many Americans will simply not seek the medical treatment that they need, nor agree to participate in health research, because they fear that their sensitive health information will be disclosed without then consent or knowledge. And those who do seek medical treatment must assume the risk of the unauthorized disclosure of their health information due to a data security breach or other privacy violation. The loss of health privacy is a growing threat to our national health care system that the Congress must address.

Senator KENNEDY and I both firmly believe that a fear of a loss of privacy cannot be allowed to deter Americans from seeking medical treatment. We are introducing this legislation today to close the privacy gap with respect to Americans' electronic health information.

A guiding principle in drafting our health privacy bill has been that the American people will only support efforts to move toward health information technology if they are assured that their sensitive health information will be protected from unauthorized disclosure and from the growing dangers of identity crimes posed by data security breaches. The bill that we are introducing today takes several important steps to honor this principle and to protect the health privacy of all Americans.

First, our bill guarantees the right of every American to privacy and security with respect to the use and disclosure of their health information. Under this legislation, every individual has the right to inspect and copy his or her own health records and to receive notice of the privacy rights and practices of data brokers and others who store this information in electronic databases. Our bill also ensures the security of electronic health information by requiring that data brokers establish safeguards to secure health information from data security breaches and other unauthorized disclosures.

Second, our bill places meaningful restrictions on the disclosure of sensitive health information. The bill expressly prohibits the disclosure or use of health information without a patient's authorization and requires that any health information intended to be used for medical research first be stripped of personally identifying information to protect an individual's privacy. There are exceptions to these restrictions for law enforcement, public safety and national security purposes.

Our bill also requires that patients be notified of a data security breach involving their health information within 15 days of discovery of the breach. The bill provides for important exceptions to this notice requirement for law enforcement and national security reasons.

Thirdly, our bill addresses the growing fear of many Americans that they will not be able to obtain important health information about a parent or child in situations involving a medical emergency, because of confusion about the requirements of current health privacy laws. The New York Times recently reported that many health care providers are overzealously applying health privacy laws, such as the Health Insurance Portability and Accountability Act, HIPAA, thwarting the legitimate efforts of family members, caretakers and even law enforcement to obtain critical health information about patients in their care. Our bill expressly allows health care providers to disclose health information to law enforcement for legitimate purposes and to a patient's next of kin, provided that the patient has been notified of their right to object to such disclosure. The bill also establishes a national office of health information privacy within the Department of Health and Human Services to aid American consumers in learning about their health privacy rights.

Lastly, our bill contains meaningful civil and criminal enforcement provisions to discourage and punish the wrongful disclosure of Americans' sensitive health information. The bill makes it a Federal crime to knowingly and intentionally disclose or use sensitive health information without an individual's consent. Violators of this provision are subject to a criminal penalty of up to $500,000 and up to 10 years in prison, if the violation is committed with the intent to sell or use sensitive health information for economic gain. In addition, the bill authorizes the Attorney General to file a civil action in Federal district court to obtain civil penalties from entities that fail to adequately safeguard electronic health records, or to provide consumers with information about their health privacy rights.

Senator KENNEDY and I have worked on this legislation for more than a decade and we both understand the need to carefully balance the right to health privacy with the legitimate needs of health care providers, medical researchers and public health and law enforcement officials. Our bill strikes the right balance between protecting privacy and ensuring public safety.

We have also conferred extensively with the many stakeholders in the health care community in crafting this legislation and our bill is supported by a wide range of public policy, consumer and health care organizations from across the political spectrum.

Senator KENNEDY and I believe that the right to health privacy is of vital interest to all Americans. For this reason, and on behalf of the millions of Americans who are currently at risk of either foregoing medical treatment or losing their right to health privacy, I urge all Senators to join us in supporting this important privacy legislation.

I ask unanimous consent that the text of the bill and a copy of the July 3, 2007, the New York Times article entitled ''Keeping Patients' Details Private, Even From Kin,'' be printed in the RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

S. 1814

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. 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 products 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 information 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 accepted scientific and statistical standards and methods for minimizing risk of disclosure; and

(iii) there is no reasonable basis to believe 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 ''decryption 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, device, equipment, or other health care-related item to an individual, or for the use of an individual, pursuant to a prescription.

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

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

(B) contractors and other health care providers 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 facilities 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 account of disclosure, use or access, that is created, accessed, received, maintained, retained, modified, recorded, stored, destroyed, or otherwise used or disclosed by a health care provider, employer, insurer, health plan, health researcher, 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 Privacy'' means the Office of Health Information Privacy designated under section 301.

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

(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, 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 otherwise holds, uses, or discloses protected health information, shall permit an individual who is the subject of such protected health information, or the individual's designee, to inspect and copy the protected health information concerning the individual, including records created under sections 102, 112, 202, 203, and 211.

(2) PROCEDURES AND FEES.—A person described 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 inspection and copying in an amount that is not in excess of the actual costs of providing such copying. Such fees may not be assessed where such an assessment would have the effect of inhibiting an individual from gaining access to the information described in paragraph (1).

(b) DEADLINE.—A person described in subsection (a)(1) shall comply with a request for inspection or copying 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 requires the inspection, copying, or sending of printed materials; or

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

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

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

(2) the person has been asked by the person described in subsection (a)(1) to fulfill the requirements of this section.

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

agreement to participate in the clinical trial.

SEC. 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.

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

(1) notify individuals whose records have been affected;

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

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

SEC. 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 authorize disclosures of protected health information, and to object to, modify, and revoke such authorizations.

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

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

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

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

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

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

(9) A statement that, if an individual elects to pay for health care from the individual's own funds, that individual may elect for identifying information not to be disclosed to anyone other than designated health care providers, unless such disclosure is 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 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) 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 safeguards and procedures for use under this section, such as, where appropriate, individual authentication of uses of computer systems, access controls, audit trails, encryption, physical security, protection of remote access points and protection of external electronic communications, periodic security assessments, incident reports, and sanctions. The 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 access, disclosure, use, or modification of protected health information;

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

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

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

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

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

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

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

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

SEC. 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 information helpful in determining the identities of such individuals) who access or seek to gain access to, use or seek to use, or disclose or seek to disclose, information sufficient to identify the protected health information sought or accessed, and other appropriate information.

(d) ACCESS TO RECORDS.—A person described in subsection (a) shall permit an individual who is the subject of protected health information, or the individual's designee, to inspect and copy the records created in paragraphs (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 disclose, access, or use protected health information except 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.

(e) 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 unauthorized 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 network or system that is used by the person.

(l) DISPOSAL OF DATA.—To prevent the unauthorized disclosure or use of protected health information, such information, when disposed of, shall be fully de-identified, 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 services.

(3) RIGHT OF HEALTH CARE PROVIDER TO REQUIRE 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, and if the withholding of services will not endanger the life of the individual, the health care provider may condition the provision of services upon the individual's execution of an 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 protected health information and no other arrangements have been made to pay for the health care services being rendered to the patient, such information may be disclosed to a governmental authority to the extent necessary to determine the individual's eligibility for, and to obtain, payment under a governmental program for health care services provided to the patient. The information may also be disclosed to another provider of health care or health care service plan as necessary to assist the other provider or health care service plan in obtaining payment for health care services rendered by that provider of health care or health care service plan to the patient.

(d) MODEL 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 this section and model statements of the limitations on authorizations. Any authorization obtained on a model authorization form under section 202 developed by the Secretary pursuant to the preceding sentence shall be deemed to satisfy the requirements of this section.

(e) SEGREGATION OF FILES.—A person described in section 102(a)(1) shall comply with the request of an individual 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 appointed 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 attached to or otherwise made a part of a coroner's or medical examiner's official report, in which case it shall no longer be protected.

(3) EXEMPTION.—Health information attached to or otherwise made a part of a coroner's or medical examiner's official report shall be exempt from the provisions of this 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 subject to the security breach, to provide the notifications required under subsection (a).

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

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—All notifications required under this section shall be made within 15 business days, or earlier if the Secretary determines appropriate, following the discovery by the person of a security breach.

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

(d) METHODS OF NOTICE.—A person described in subsection (a) shall provide to an

individual the following forms of notice in the case of a security breach:

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

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

(B) telephone notice to the individual personally; or

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

(2) MEDIA NOTICE.—Notice shall be provided to prominent media outlets serving a State or jurisdiction, if the 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 information that has been, or is reasonably believed to have been, accessed, disclosed, or otherwise used by an unauthorized person;

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

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

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

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

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

(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 deidentified 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 prevention of injury, disease, or premature mortality, or the promotion of health, in a community, including—

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

(2) implementing public health policy;

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

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

(c) LIMITATIONS.—The purpose of the disclosure described in subsection (a) 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 creates, accesses, maintains, retains, modifies, records, stores, destroys, or otherwise uses or discloses protected health information under this title may disclose such information to a protection and advocacy agency established under part C of title I of the Developmental Disabilities Assistance and Bill of Rights Act (42 U.S.C. 6041 et seq.) or under the Protection and Advocacy for Mentally Ill Individuals Act of 1986 (42 U.S.C. 10801 et seq.) when such person 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.

(e) 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 reasonably be satisfied by de-identified 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) 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 voluminous or if compliance with such order otherwise would cause an unreasonable burden on such entities.

(d) 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 prior 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 prior notice to the individual if the court finds 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, intelligence, counter-intelligence, or other national security information.

(e) 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.

(f) LIMITATION ON USE AND DISCLOSURE FOR NATIONAL SECURITY, INTELLIGENCE, AND 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 entity for use in, any administrative, civil, or criminal action or investigation directed against the individual, unless the action or investigation arises out of, or is directly related to, the law enforcement, national security, or intelligence inquiry for which the information was obtained.

(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 research under this section shall provide the Secretary with the names and addresses of the institutional review board members.

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

(C) MONITORING.—The Secretary shall periodically monitor institutional review boards described in this subsection.

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

(g) LIMITATION.—Nothing in this section shall be construed to permit 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 information.

SEC. 218. JUDICIAL AND ADMINISTRATIVE PURPOSES.

(a) IN GENERAL.—A person described in section 102(a)(1), or a 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 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 information 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 application regarding the provision of treatment of an individual 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.

(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 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 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) 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, insurer, health or life insurer, school or university, agent, or other person involved with a signed document attesting—

(A) 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

(B) the date on which the individual or the individual's attorney was notified under paragraph (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 interest of the individual by—

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

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

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

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

(d) RIGHTS OF MINORS.—

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

(A) who is 18 years of age or older, all rights of the individual under this 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.

(e) 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.

(c) STANDARDS FOR CERTIFICATION.—

(1) ESTABLISHMENT.—Not later than 12 months after the date of enactment of this Act, the Secretary, in consultation with the Director of the Office and the Director of the Office of Civil Rights, shall establish and implement standards for health information technology products 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 technology 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 subsection (b) shall apply to a person that knowingly and intentionally—

''(1) obtains, uses, or attempts to obtain or use protected health information relating to an individual in violation of title II of the Health Information 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 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 or imprisoned 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 malicious harm, be fined not more than $500,000, imprisoned not more than 10 years, or any combination of such penalties.

''(c) SUBSEQUENT OFFENSES.—In the case of a person described in subsection (a), the maximum penalties described in subsection (b) shall be doubled for every subsequent conviction for an offense arising out of a violation or violations related to a set of circumstances that are different 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 following new item:

''Sec. 2801. Wrongful disclosure of protected health information.''

SEC. 312. DEBARMENT FOR CRIMES AND CIVIL VIOLATIONS.

(a) PURPOSE.—The purpose of this section is to prevent 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 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 regulations 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 imposed 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 statement or obstructing justice related to attempting 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 debarment imposed under this section to take into account the medical needs of patients.

(c) 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 regarding 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 offenses, 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 imposed 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 resides, 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 engagement of a person in a practice that is prohibited under this subtitle, the State or local law enforcement agency on behalf of the residents of the agency's jurisdiction, may bring a civil action on behalf of the residents of the State or jurisdiction in a district court of the United States of appropriate jurisdiction to—

(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 action under paragraph (1), the attorney general of the State involved shall provide to the Attorney General and Secretary—

(i) written notice of the action; and

(ii) a copy of the complaint for the action.

(B) EXEMPTION.—Subparagraph (A) shall not apply with respect to the filing of an action by a State attorney general under this subsection, if the attorney general of a State determines that it is not feasible to provide the notice 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 consultation with the Secretary, shall, have the right to—

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

(2) intervene in an action brought under subsection (a)(2); and

(3) file petitions for appeal.

(c) PENDING PROCEEDINGS.—If the Attorney General 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 proceeding 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 proceeding 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 subsection (a) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

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

(A) is an inhabitant; or

(B) may be found.

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 discriminate or cause any employer to discriminate against an employee 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 violation of this Act by an employer or an employee of an employer.

(b) ENFORCEMENT ACTIONS.—

(1) IN GENERAL.—Any employee or former employee 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 Fair Labor Standards Act of 1938 (29 U.S.C. 203(g)) for the purposes of implementing the requirements of that Act (29 U.S.C. 201, et seq.).

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

(3) EMPLOYER.—The term ''employer'' means any person who employs employees, including any person acting directly or indirectly in the interest of any employer in relation to an employee and includes a public agency.

(g) GENERAL PROHIBITION AGAINST RETALIATION.—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 assisted, 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.

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

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

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

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

(4) governs a minor's rights to access 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 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.

KEEPING PATIENTS' DETAILS PRIVATE, EVEN FROM KIN

(By Jane Gross)

An emergency room nurse in Palos Heights, Ill., told Gerard Nussbaum he could not stay with his father-in-law while the elderly man was being treated after a stroke. Another nurse threatened Mr. Nussbaum with arrest for scanning his relative's medical chart to prove to her that she was about to administer a dangerous second round of sedatives.

The nurses who threatened him with eviction and arrest both made the same claim, Mr. Nussbaum said: that access to his father-in-law and his medical information were prohibited under the Health Insurance Portability and Accountability Act, or Hipaa, as the federal law is known.

Mr. Nussbaum, a health care and Hipaa consultant, knew better and stood his ground. Nothing in the law prevented his involvement. But the confrontation drove home the way Hipaa is misunderstood by medical professionals, as well as the frustration—and even peril—that comes in its wake.

Government studies released in the last few months show the frustration is widespread, an unintended consequence of the 1996 law.

Hipaa was designed to allow Americans to take their health insurance coverage with them when they changed jobs, with provisions to keep medical information confidential. But new studies have found that some health care providers apply Hipaa regulations overzealously, leaving family members, caretakers, public health and law enforcement authorities stymied in their efforts to get information.

Experts say many providers do not understand the law, have not trained their staff members to apply it judiciously, or are fearful of the threat of fines and jail terms—although no penalty has been levied in four years.

Some reports blame the language of the law itself, which says health care providers may share information with others unless the patient objects, but does not require them to do so. Thus, disclosures are voluntary and health care providers are left with broad discretion.

The unnecessary secrecy is a ''significant problem,'' said Mark Rothstein, chairman of a privacy subcommittee that advises the Department of Health and Human Services, which administers Hipaa. ''It's drummed into them that there are rules they have to follow without any perspective,'' he said about health care providers. ''So, surprise, surprise, they approach it in a defensive, somewhat arbitrary and unreasonable way.''

Susan McAndrew, deputy director of health information privacy at the Department of Health and Human Services, said that problems were less frequent than they once had been but that health care providers continued to hide behind the law. ''Either innocently or purposefully, entities often use this as an excuse,'' she said. ''They say 'Hipaa made me do it' when, in fact, they chose for other reasons not to make the permitted disclosures.''

Mr. Rothstein, one of Hipaa's harshest critics, has led years of hearings across the country. Transcripts of those hearings, and accounts from hospital administrators, patient advocates, lawyers, family members, and law enforcement officials offer an anthology of Hipaa misinterpretations, some alarming, some annoying:

Birthday parties in nursing homes in New York and Arizona have been canceled for fear that revealing a resident's date of birth could be a violation.

Patients were assigned code names in doctor's waiting rooms—say, ''Zebra'' for a child in Newton, Mass., or ''Elvis'' for an adult in Kansas City, Mo.—so they could be summoned without identification.

Nurses in an emergency room at St. Elizabeth Health Center in Youngstown, Ohio, refused to telephone parents of ailing students themselves, insisting a friend do it, for fear of passing out confidential information, the hospital's patient advocate said.

State health departments throughout the country have been slowed in their efforts to create immunization registries for children, according to Dr. James J. Gibson, the director of disease control in South Carolina, because information from doctors no longer flows freely.

Teaching staff to protect records is easier than teaching them to share them, said Robert N. Swidler, general counsel for Northeast Health, a nonprofit network in Troy, N.Y., that includes several hospitals.

''Over time, the staff has become a little more flexible and humane,'' Mr. Swidler said. ''But nurses aren't lawyers. This is a hyper-technical law and it tells them they may disclose but doesn't say they have to.''

Many experts, including critics like Mr. Rothstein and proponents like Ms. McAndrew, distinguish different categories of secrecy.

There are ''good faith nondisclosures,'' as when a floor nurse takes a phone call from someone claiming to be a family member but cannot verify that person's identity. Then there are ''bad faith nondisclosures,'' like using Hipaa as an excuse for not taking the time to gather records that public health officials need to help child abuse investigators trying to build a case.

Most common are seat-of-the-pants decisions made by employees who feel safer saying ''no'' than ''yes'' in the face of ambiguity.

That seemed to be what happened to his own mother, Mr. Rothstein said, when she called her doctor's office to discuss a problem. She was told by the receptionist that the doctor was not available, Mr. Rothstein said, and then inquired if the doctor was with a patient or out of the office. ''I can't tell you because of Hipaa,'' came the reply. In fact the doctor was home sick, which would have been helpful information in deciding whether to wait for a call back or head for the emergency room.

The law, medical professionals and privacy experts said, has had the positive effect of making confidentiality a priority as the nation moves toward fully computerized, cradle-to-grave medical records.

But safeguarding electronic privacy required a tangle of regulations issued in 2003, followed last year by 101 pages of ''administrative simplification.''

Senator Edward M. Kennedy, Democrat of Massachusetts, a sponsor of the original insurance portability law, was dismayed by the ''bizarre hodgepodge'' of regulations layered onto it, several staff members said, and by the department's failure to provide ''adequate guidance on what is and is not barred by the law.'' To that end, Mr. Kennedy, along with Senator Patrick M. Leahy, Democrat of Vermont, plans to introduce legislation creating an office within the Department of Health and Human Services dedicated to interpreting and enforcing medical privacy.

''In this electronic era it is essential to safeguard the privacy of medical records while insuring our privacy laws do not stifle the flow of information fundamental to effective health care,'' Mr. Kennedy said.

This spring, the department revised its Web site, www.hhs.gov/ocr/hipaa, in the interest of clarity. But Hipaa continues to baffle even the experts.

Ms. McAndrew explained some of the do's and don'ts of sharing information in a telephone interview:

Medical professionals can talk freely to family and friends, unless the patient objects. No signed authorization is necessary and the person receiving the information need not have the legal standing of, say, a health care proxy or power of attorney. As for public health authorities or those investigating crimes like child abuse, Hipaa defers to state laws, which often, though not always, require such disclosure. Medical workers may not reveal confidential information about a patient or case to reporters, but they can discuss general health issues.

Ms. McAndrew said there was no way to know how often information was withheld. Of the 27,778 privacy complaints filed since 2003, the only cases investigated, she said, were complaints filed by patients who were denied access to their own information, the one unambiguous violation of the law.

Complaints not investigated include the plights of adult children looking after their parents from afar. Experts say family members frequently hear, ''I can't tell you that because of Hipaa,'' when they call to check on the patient's condition.

That is what happened to Nancy Banks, who drove from Bartlesville, Okla., to her mother's bedside at Town and Country Hospital in Tampa, Fla., last week because Ms. Banks could not find out what she needed to know over the telephone.

Her 82-year-old mother had had a stroke. When Ms. Banks called her room she heard her mother ''screaming and yelling and crying,'' but conversation was impossible. So Ms. Banks tried the nursing station.

Whoever answered the phone was not helpful, so Ms. Banks hit the road. Twenty-two hours later, she arrived at the hospital.

But more of the same awaited her. She said her mother's nurse told her that ''because of the Hipaa laws I can get in trouble if I tell you anything.''

In the morning, she could speak to the doctor, she was told.

The next day, Ms. Banks was finally informed that her mother had had heart failure and that her kidneys were shutting down.

''I understand privacy laws, but this has gone too far,'' Ms. Banks said. ''I'm her daughter. This isn't right.''

A hospital spokeswoman, Elena Mesa, was asked if nurses were following Hipaa protocol when they denied adult children information about their parents.

She could not answer the question, Ms. Mesa said, because Hipaa prevented her from such discussions with the press.

Mr. KENNEDY. Mr. President, it is a privilege to join my friend and colleague Senator LEAHY in introducing the Protection of Health Information Privacy and Security Act of 2006. Protecting the privacy of patients' health information is a major priority in health reform, and I look forward to the enactment of this legislation to do so.

In 1996, the Senate enacted HIPAA, the Health Insurance Portability and Accountability Act, which I introduced with Senator Kassebaum. That law gave Americans the ability to continue their health insurance when they changed jobs. It has become clear, however, that the privacy rules under the act have not succeeded in protecting patients adequately.

Since HIPAA became law, numerous privacy bills to protect personal health information have been introduced in Congress, but none of them has been enacted.

In fact, the HIPAA law required the Secretary of Health and Human Services to develop privacy regulations if Congress failed to enact privacy rules by August 1999. When Congress did not act, the Department of Health and Human Services prescribed privacy rules, but its authority to do so under HIPAA was limited to regulating only the privacy-related activities of three specific ''covered entities,'' health care providers, payers, and clearinghouses. Other entities, such as schools, employers, and health agencies, can be regulated only indirectly, as business associates of covered entities, even though many of them also possess confidential health data.

This indirect oversight has made it very difficult to enforce implementation of the Department's safeguards for entities other than the three specifically listed in the HIPAA privacy rule. The result is that Americans continue to be at risk of having their personal medical records and other confidential health information wrongly distributed and exposed without their authorization, and often even without their knowledge.

One common problem involves domestic and offshore outsourcing. HIPAA-covered entities and business associates can hire outside companies, either in the U.S. or in other countries, to do work for them. The tasks of those outside companies may require them to obtain personal health information. There is widespread concern, however, that once this private information leaves the original holder, the legitimacy of any subsequent disclosure of it becomes much more difficult to enforce.

Obviously, we need to revise our approach to health information privacy in order to protect the rights of those who rely on their doctors and their Government to safeguard their private information.

The pending health information technology bill, S. 1693, was the subject of much discussion on this issue. Some feel that the bill should include more extensive privacy regulations than it does. But that measure is not the best vehicle to restructure health-information privacy. Attempting to rewrite privacy rules through health IT legislation would be a piecemeal approach to correcting the shortcomings of privacy protections. The Health Information Privacy and Security Act presents an opportunity to make comprehensive improvements to health privacy protections. Addressing health information privacy through this legislation will ensure the security of patients' information, in any form, electronic or otherwise.

The bill that Senator LEAHY and I are introducing today corrects the longstanding errors in the ways in which confidential patient information is handled and distributed. We live in a time when Americans are increasingly aware of breaches of their privacy. It is essential for us to enact effective reforms to protect all Americans from further infringements on their health privacy.

The system now in place allows much of importance to fall through the cracks. Enforcement has been inadequate. The Office for Civil Rights of the Department of Health and Human Services, which is responsible for the enforcement of HIPAA, has received more than 20,000 complaints, but it has not imposed any civil penalties in response. The Department of Justice has effectively prosecuted only four criminal violations of HIPAA.

A few examples illustrate the problem. In June 2006, the Centers for Medicare and Medicaid reported that the health information of 17,000 Americans whose insurance plans are provided by Humana, Inc. was at risk because of unsecured computer data. Last September, the Government Accountability Office urged Medicare to implement stronger oversight over the transmission of private health records. A GAO survey had found that almost half of all responding Medicare Advantage contractors admitted to recent breaches of privacy of health records. In addition, the number of health plan providers that identified themselves as ''mostly compliant'' with HIPAA's privacy regulations decreased from 91 percent in 2005 to 85 percent in 2006. These findings demonstrate that patients' right to know and authorize who views their medical information is being neglected.

Americans live in a democracy where they believe, rightly, that they themselves should have the power to decide when, and to whom, their health information is disclosed. The bill we are introducing today will better enable Federal privacy rules to fulfill that expectation.

This bill complements and strengthens Federal privacy regulations by adding more effective oversight and individuals' access to their own personal information. It requires the Secretary of the Department of Health and Human Services to revise the HIPAA Privacy Rule to make it consistent with this act.

The bill gives each American the full ability to obtain and modify any of their health records, whether the records are carried by one of the HIPAA Privacy Rule's three ''covered entities'' or by any other entity. Except in rare cases, authorization by an individual is required before any other person or entity can disclose, obtain, or use that individual's protected health information.

The bill also addresses the existing outsourcing problem by improving transparency. Any entity that entrusts outside agents or overseas providers with personal health information must publish their names and ensure that they abide by the required privacy and security measures.

The act requires all entities that deal with protected health information in any way to implement safeguards to protect that information. Such entities must also maintain safeguards that are up-to-date with current technology.

Any entity that possesses or obtains an individual's protected health information is required to give that individual a notice of privacy rights and practices, including the individual's right to be alerted if a security breach concerning the information occurs. Individuals are also promised a clear description of who will have access to their personal health information and how the information will be used. In this way, people will always be aware of what is going on with their private information. They will feel more secure about it, and be more secure.

The bill also establishes a demonstration grant program to help those who have low health literacy or limited english-language proficiency to exercise their privacy rights and avoid cultural or linguistic barriers.

This Act also creates a new office in the Department of Health and Human Services, the Office of Health Information Privacy, which will oversee investigations of alleged violations and verify compliance with the act. This office will also be responsible for establishing and implementing standards and product certifications for systems and networks that handle protected health information. Until now, many entities have been confused about how to implement health privacy regulations. This new office will help them understand Federal privacy rules, so that they can conduct their business accordingly.

Federal privacy regulations now in place also make it difficult to prosecute illegal activities. The Office of Health Information Privacy will be charged with resolving this problem. It will do so in part by instituting penalties for wrongful sharing or use of private health information by any entity.

Overall, a delicate balance must be struck. On one hand, we must allow the sharing of information necessary for effective health care. At the same time, however, we must protect Americans' right to have their health records and individual health information kept private. For too long, the balance has been tilted too far against patient privacy, and our bill is a needed effort to correct that imbalance.

Americans deserve stronger guarantees of patient privacy, more helpful guidelines for security implementation, and more dependable enforcement and penalties for the misuse of protected health information. I look forward to the early enactment of this legislation to achieve these important goals.

SUBMITTED RESOLUTIONS

SENATE RESOLUTION 274—TO AUTHORIZE REPRESENTATION BY THE SENATE LEGAL COUNSEL IN THE CASE OF LEWIS V. BAYH

Mr. REID (for himself and Mr. MCCONNELL) submitted the following resolution; which was considered and agreed to:

S. RES. 274

Whereas, in the case of Lewis v. Bayh, Case No. 07–CV–0939 (D.D.C.), pending in the United States District Court for the District of Columbia, the plaintiff has named as defendant Senator Evan Bayh;

Whereas, pursuant to sections 703(a) and 704(a)(1) of the Ethics in Government Act of 1978, 2 U.S.C. §§288b(a) and 288c(a)(1), the Senate may direct its counsel to defend the Senate and Members, officers, and employees of the Senate in civil actions relating to their official responsibilities; Now therefore, be it

Resolved, That the Senate Legal Counsel is authorized to represent Senator Evan Bayh in the case of Lewis v. Bayh.

SENATE RESOLUTION 275—MAKING MINORITY PARTY APPOINTMENTS FOR THE 110TH CONGRESS

Mr. MCCONNELL submitted the following resolution; which was considered and agreed to:

S. RES. 275

Resolved, That the following be the minority membership on the Committee on Armed Services for the remainder of the 110th Congress, or until their successors are appointed:

Mr. McCain, Mr. Warner, Mr. Inhofe, Mr. Sessions, Ms. Collins, Mr. Chambliss, Mr. Graham, Mrs. Dole, Mr. Cornyn, Mr. Thune, Mr. Martinez, and Mr. Corker.

AMENDMENTS SUBMITTED AND PROPOSED

SA 2314. Mr. REID submitted an amendment intended to be proposed by him to the bill H.R. 2669, to provide for reconciliation pursuant to section 601 of the concurrent resolution on the budget for fiscal year 2008; which was ordered to lie on the table.

SA 2315. Mr. DORGAN submitted an amendment intended to be proposed by him to the bill H.R. 1585, to authorize appropriations for fiscal year 2008 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table.

SA 2316. Mr. BUNNING submitted an amendment intended to be proposed by him to the bill H.R. 1585, supra; which was ordered to lie on the table.

SA 2317. Mr. SESSIONS submitted an amendment intended to be proposed by him to the bill H.R. 1585, supra; which was ordered to lie on the table.

SA 2318. Mr. SESSIONS submitted an amendment intended to be proposed by him to the bill H.R. 1585, supra; which was ordered to lie on the table.

SA 2319. Mr. SESSIONS submitted an amendment intended to be proposed by him to the bill H.R. 1585, supra; which was ordered to lie on the table.

SA 2320. Mr. SMITH (for himself and Mr. WYDEN) submitted an amendment intended to be proposed by him to the bill H.R. 1585, supra; which was ordered to lie on the table.

SA 2321. Mrs. DOLE submitted an amendment intended to be proposed by her to the bill H.R. 1585, supra; which was ordered to lie on the table.

SA 2322. Mr. KYL (for himself and Mr. DOMENICI) submitted an amendment intended to be proposed by him to the bill H.R. 1585, supra; which was ordered to lie on the table.

SA 2323. Mr. KERRY (for himself and Ms. SNOWE) submitted an amendment intended to be proposed by him to the bill H.R. 1585, supra; which was ordered to lie on the table.

SA 2324. Mr. HAGEL (for himself and Mr. BYRD) submitted an amendment intended to be proposed by him to the bill H.R. 1585, supra; which was ordered to lie on the table.

SA 2325. Mr. BAUCUS (for himself and Mr. TESTER) submitted an amendment intended to be proposed by him to the bill H.R. 1585, supra; which was ordered to lie on the table.

SA 2326. Mr. CARDIN (for himself, Mr. BIDEN, Mr. STEVENS, Mr. BAYH, Mrs. CLINTON, Ms. MIKULSKI, Ms. MURKOWSKI, Mr. KERRY, Mr. VITTER, Mr. ISAKSON, Mr. LAUTENBERG, and Mr. KENNEDY) submitted an amendment intended to be proposed by him to the bill H.R. 1585, supra; which was ordered to lie on the table.

SA 2327. Mr. KENNEDY proposed an amendment to the bill H.R. 2669, to provide for reconciliation pursuant to section 601 of the concurrent resolution on the budget for fiscal year 2008.

SA 2328. Mr. REID submitted an amendment intended to be proposed by him to the bill S. 1642, to extend the authorization of programs under the Higher Education Act of 1965, and for other purposes; which was ordered to lie on the table.

SA 2329. Ms. MURKOWSKI proposed an amendment to amendment SA 2327 proposed by Mr. KENNEDY to the bill H.R. 2669, to provide for reconciliation pursuant to section 601 of the concurrent resolution on the budget for fiscal year 2008.

SA 2330. Mr. KENNEDY proposed an amendment to amendment SA 2327 proposed by Mr. KENNEDY to the bill H.R. 2669, supra.

TEXT OF AMENDMENTS

SA 2314. Mr. REID submitted an amendment intended to be proposed by him to the bill H.R. 2669, to provide for reconciliation pursuant to section 601 of the concurrent resolution on the budget for fiscal year 2008; which was ordered to lie on the table; as follows:

At the end of the bill, add the following:

SEC. 802. CAMPUS-BASED DIGITAL THEFT PREVENTION.

Part G of title IV (20 U.S.C. 1088 et seq.) is amended by adding at the end the following:

"SEC. 494. CAMPUS-BASED DIGITAL THEFT PREVENTION.

''(a) IN GENERAL.—Each eligible institution participating in any program under this title which is among those identified during the prior calendar year by the Secretary pursuant to subsection (b)(2), shall—

''(1) provide evidence to the Secretary that the institution has notified students on its policies and procedures related to the illegal downloading and distribution of copyrighted materials by students as required under section 485(a)(1)(P);

''(2) undertake a review, which shall be submitted to the Secretary, of its procedures and plans related to preventing illegal downloading and distribution to determine the program's effectiveness and implement changes to the program if the changes are needed; and

''(3) provide evidence to the Secretary that the institution has developed a plan for implementing a technology-based deterrent to prevent the illegal downloading or peer-to-peer distribution of intellectual property.

''(b) IDENTIFICATION.—For purposes of carrying out the requirements of subsection (a), the Secretary shall, on an annual basis, identify—

''(1) the 25 institutions of higher education participating in programs under this title, which have received during the previous calendar year the highest number of written notices from copyright owners, or persons authorized to act on behalf of copyright owners, alleging infringement of copyright by users of the institution's information technology systems, where such notices identify with specificity the works alleged to be infringed, or a representative list of works alleged to be infringed, the date and time of the alleged infringing conduct together with information sufficient to identify the infringing user, and information sufficient to contact the copyright owner or its authorized representative; and

''(2) from among the 25 institutions described in paragraph (1), those that have received during the previous calendar year not less than 100 notices alleging infringement of