HEALTH INFORMATION PRIVACY MODEL ACT

Table of Contents

Section 1. Title

This Act may be known and shall be cited as the Health Information Privacy Act.

Section 2. Purpose

The purpose of this Act is to set standards to protect health information from unauthorized collection, use and disclosure by requiring carriers to establish procedures for the treatment of all health information.

Section 3. Definitions

As used in this Act:

A. "Carrier" means a person or entity required to be licensed or authorized by the commissioner to assume risk, including but not limited to an insurer, a hospital, medical or health service corporation, a health maintenance organization, a provider sponsored organization, a multiple employer welfare arrangement, a self-insured group fund or a workers' compensation self-insurer. Carrier does not include a non-risk-bearing regulated insurance entity, such as a producer, agency or administrator.

Drafting Note: Some entities that collect, use or disclose protected health information may not be subject to the jurisdiction of the insurance commissioner, but may be subject to the jurisdiction of another state agency, such as the Department of Labor or the Department of Health. States may want to ensure fair and equitable regulation of all entities that collect, use or disclose protected health information by making parallel amendments to other appropriate state laws, such as workers' compensation laws.

B. "Commissioner" means the insurance commissioner of this state.

Drafting Note: Use the title of the chief insurance regulatory official wherever the term "commissioner" appears. If the jurisdiction of certain health carriers, such as health maintenance organizations, lies with some state agency other than the insurance department, or if there is dual regulation, a state should add language referencing that agency to ensure the appropriate coordination of responsibilities.

C. "Covered person" means a policyholder, subscriber, enrollee, beneficiary, insured, certificateholder or other person covered by a policy, contract or agreement of insurance issued by a carrier.

D. "Disclose" means to release, transfer, or otherwise divulge protected health information to any person other than to the individual who is the subject of the protected health information.

E. "Facility" means an institution providing health care services or a health care setting, including but not limited to hospitals and other licensed inpatient centers, ambulatory surgical or treatment centers, skilled nursing centers, residential treatment centers, diagnostic, laboratory and imaging centers, and rehabilitation and other therapeutic health settings.

F. "Health care" means:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, services, procedures, tests, or counseling that:

(a) Relates to the physical, mental or behavioral condition of an individual; or

(b) Affects the structure or function of the human body or any part of the human body, including the banking of blood, sperm, organs, or any other tissue; or

(2) Prescribing, dispensing, or furnishing to an individual drugs or biologicals, or medical devices or health care equipment and supplies.

G. "Health care professional" means a physician or other health care practitioner licensed, accredited or certified to perform specified health services consistent with state law.

H. "Health care provider" or "provider" means a health care professional or facility.

I. "Health information" means any information or data, whether oral or recorded in any form or medium, and personal facts or information about events or relationships that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of an individual or a member of the individual's family;

(2) The provision of health care to an individual; or

(3) Payment for the provision of health care to an individual.

J. "Insurance support organization" means a person that regularly engages, in whole or in part, in the practice of assembling or collecting information from carriers, agents or other insurance support organizations for the purpose of ratemaking or ratemaking-related functions, regulatory or legislative cost analysis, detecting or preventing fraud, material misrepresentation or material nondisclosure in connection with insurance underwriting or insurance claim activity. Persons that are not considered "insurance support organizations" for purposes of this Act are agents, government institutions, insurance institutions, medical care institutions and medical professionals.

Drafting Note: States may wish to include either separately or in the definition section, a definition of the term "insurance institution," from the NAIC Insurance Information and Privacy Protection Model Act. "Insurance institution" means any corporation, association, partnership, reciprocal exchange, inter-insurer, Lloyd's insurer, fraternal benefit society or other person engaged in the business of insurance, including health maintenance organizations, medical service plans and hospital service plans as defined in [insert applicable section of the State insurance code which defines health maintenance organization or medical or hospital service plans.]

K. "Person" means an individual, a corporation, a partnership, an association, a joint venture, a joint stock company, a trust, an unincorporated organization, any similar entity or a combination of the foregoing.

L. "Protected health information" means health information:

(1) That identifies an individual who is the subject of the information; or

(2) With respect to which there is a reasonable basis to believe that the information could be used to identify an individual.

M. "Research" means the process of systematic investigation or inquiry including, but not limited to any of the following: the systematic development and testing of a hypothesis; and the systematic description, analysis and measurement of processes, behaviors and physical, social, political, or medical phenomena.

N. "Research organization" means a person or organization, other than the carrier disclosing the protected health information, engaged in research.

O. (1) "Scientific, medical or public policy research" means research conducted to improve the effectiveness of:

(a) Determining medical causation, diagnosis and treatment;

(b) Public health; or

(c) The operations of the public or private health care, insurance or workers' compensation systems; and

(2) (a) The results of the research are intended for publication;

(b) The research findings are intended to be widely disseminated beyond the carrier and research organization so as to benefit the public good; and

(3) The scientific, medical or public policy research excludes all activities listed in Section 10H(1).

P. "Unauthorized" means a collection, use or disclosure of protected health information made by a carrier without the authorization of the subject of that protected health information or that is not in compliance with this Act, unless collection, use or disclosure without an authorization is permitted by this Act.

Section 4. Applicability and Scope

This Act applies to all carriers and governs the management of health information, including the collection, use, and disclosure of protected health information by carriers.

Section 5. Health Information Policies, Standards and Procedures

A. A carrier shall develop and implement written policies, standards and procedures for the management of health information, including policies, standards and procedures to guard against the unauthorized collection, use or disclosure of protected health information by the carrier which shall include:

(1) Limitation on access to health information by only those persons who need to use the health information in order to perform their jobs;

(2) Appropriate training for all employees;

(3) Disciplinary measures for violations of the health information policies, standards and procedures;

(4) Identification of the job titles and job descriptions of persons that are authorized to disclose protected health information;

(5) Procedures for authorizing and restricting the collection, use or disclosure of protected health information;

(6) Methods for exercising the right to access and amend protected health information as provided in Sections 7 and 8;

(7) Methods for handling, disclosing, storing and disposing of health information;

(8) Periodic monitoring of the employees' compliance with the carrier's policies, standards and procedures in a manner sufficient for the carrier to determine compliance with this Act and to enforce its policies, standards and procedures; and

(9) Methods for informing and allowing an individual who is the subject of protected health information to request specialized disclosure or nondisclosure of protected health information as required under Section 14.

B. (1) In any contractual arrangement between a carrier and a person other than a covered person or health care provider where the person collects or uses protected health information on behalf of the carrier or where the carrier discloses protected health information to the person a carrier shall:

(a) Require the person to have health information policies, standards and procedures that comply with the requirements of this Act; and

(b) Inform the person of its obligation to comply with any applicable state and federal statutory and regulatory requirements governing the collection, use or disclosure of protected health information.

(2) In any contractual arrangement between a carrier and a health care provider, a carrier shall require that the health care provider have health information privacy policies, standards and procedures.

(3) Notwithstanding Section 18, all contractual arrangements described in this subsection in effect on [insert effective date], shall comply with this Act no later than eighteen (18) months after [insert effective date] or the renewal date of the contract, whichever is earlier.

C. A carrier shall make the health information policies, standards and procedures developed pursuant to this section available for review by the commissioner.

Section 6. Notice of Health Information Policies, Standards and Procedures

A. A carrier shall draft a written notice of its health information policies, standards and procedures developed pursuant to Section 5, which shall be made available for review by the commissioner. The notice shall include:

(1) The collection, use and disclosure of protected health information prohibited and permitted by this Act;

(2) The procedures for authorizing and limiting disclosures of protected health information and for revoking authorizations;

(3) The procedures for accessing and amending protected health information; and

(4) The right of a covered person to review a copy of the carrier's health information policies, standards and procedures.

B. The carrier shall provide the notice to any person upon request, to covered persons at the time the policy is first delivered, and to all other individuals when requesting an authorization. If subsequent policies are issued to the same insured, no additional notices are required to be included when those subsequent policies are delivered.

Drafting Note: The language regarding subsequent policies is meant to clarify that notice does not need to be redelivered every time changes are made to the policy a carrier has with an existing policyholder. For example, notice need not be redelivered when an automobile is added to an automobile insurance policy.

Section 7. Right to Access Protected Health Information

A. Subject to the exceptions listed in Subsection B(3) of this section, an individual who is the subject of the protected health information has the right to examine or receive a copy of the protected health information that is in the possession of the carrier or a person acting on behalf of the carrier.

B. No later than twenty (20) working days after receipt of a written request for protected health information from an individual who is the subject of protected health information, a carrier shall do one of the following:

(1) Provide a copy of the protected health information requested to the individual or if providing a copy is not possible, permit the individual to examine the protected health information during regular business hours;

(2) Notify the individual that the carrier does not have the protected health information and, if known, inform the individual of the name and address of the person who has the protected health information requested or, if the carrier will be obtaining access to the requested protected health information, when the protected health information is expected to be available to the individual; or

(3) Deny the request in whole or in part if the carrier determines any of the following:

(a) Knowledge of the protected health information would reasonably be expected to identify a confidential source who provided the protected health information in conjunction with a lawfully conducted investigation, law enforcement investigation, or court proceeding;

(b) The protected health information was compiled in preparation for litigation, law enforcement or fraud investigation, quality assurance or peer review purposes;

(c) The protected health information is the original work product of the carrier, which would include but not be limited to interpretation, mental impressions, instructions and other original product of the carrier, its employees and agents;

(d) The requester is a party to a legal proceeding involving the carrier where the health condition of the requester is at issue. However, once a legal proceeding is resolved, the individual's right to access protected health information under this section and to amend protected health information under Section 8 shall be restored; or

(e) Disclosure of the protected health information to the individual who is the subject of the protected health information is otherwise prohibited by law.

C. If a request to examine or copy protected health information is denied in whole or in part under this section, the carrier shall notify the individual who is the subject of the protected health information of the reasons for the denial in writing. When the protected health information was compiled in preparation for litigation, law enforcement or fraud investigation, the carrier is not required to notify the individual of the reasons for the denial.

Drafting Note: When the information that has been requested is not subject to release, the carrier should inform the requester that all information required to be released under this Act has been released.

D. A carrier is not required to create a new record or reformulate an existing record in order to meet a request for protected health information.

E. The carrier may charge a reasonable fee for providing the protected health information requested and shall provide a detailed bill accounting for the charges. No charge shall be made for reproduction of protected health information requested for the purpose of supporting a claim, supporting an appeal or accessing any federal or state sponsored or operated health benefits program.

Section 8. Right to Amend Protected Health Information

A. An individual who is the subject of protected health information has the right to amend the protected health information to correct any inaccuracies.

B. Within thirty (30) working days after receipt of a written request from an individual who is the subject of protected health information to amend protected health information, a carrier shall act to verify the accuracy of protected health information identified as erroneous by the individual and shall do one of the following:

(1) Correct or amend (either by changing the information in question or adding additional information as provided by the individual), or delete the portion of the protected health information in dispute and notify the individual of the changes; or

(2) Notify the individual that the request has been denied, the reason for the denial, and that the individual may:

(a) Request that the health care provider who created the record in question amend the record. The carrier shall include the health care provider's name and address; or

(b) File a concise statement of what the individual believes to be the correct information and the reasons why the individual disagrees with the denial. The carrier shall retain this statement filed by the individual with the protected health information.

C. If the carrier corrects, amends or deletes the protected health information as requested pursuant to Subsection B(1), the carrier shall furnish the correction, amendment or deletion to:

(1) All persons who have received the protected health information that has been corrected, amended or deleted from the carrier within the preceding two (2) years;

(2) An insurance support organization whose primary source of protected health information is carriers, as long as the insurance support organization has systematically received protected health information from the carrier within the preceding seven (7) years. However, the correction, amendment or deletion need not be furnished if the insurance support organization no longer maintains the protected health information that has been corrected, amended or deleted; and

(3) Any person that furnished the protected health information that was amended pursuant to Subsection B(1).

D. If the individual who is the subject of the protected health information files a statement pursuant to Subsection B(2)(b), the carrier shall:

(1) Clearly identify the matter or matters in dispute and include the statement in any subsequent disclosure of the protected health information; and

(2) Furnish the statement to the persons described in Subsection C.

E. Nothing in this section shall require a carrier to alter, delete, erase or obliterate medical records provided to them by a health care provider.

F. Nothing in this section shall be construed to give a person access to protected health information covered by the exceptions listed in Section 7B(3).

Section 9. List of Disclosures of Protected Health Information

A. A carrier shall provide upon request, to an individual who is the subject of the protected health information, information regarding disclosure of that individual's protected health information that is sufficient to exercise the right to amend the information pursuant to Section 8. This information shall include the date, purpose, recipient and relevant authorization or basis for the disclosure. The carrier may charge a reasonable fee for providing the information regarding the disclosures of information.

B. A carrier shall maintain a system that is sufficient for the commissioner to determine that the carrier can produce a complete list of disclosures.

(1) For routine disclosures, a carrier shall be able to track when routine disclosures are made, to whom they are made and for what purpose they are made; and

(2) For all other disclosures, a carrier shall be able to identify the authorization or release form or provision of law allowing the receipt or disclosure of protected health information.

C. A carrier is not required to include in the information developed pursuant to Section 9A any disclosures of protected health information that were compiled in preparation for litigation, law enforcement or fraud investigation.

Section 10. Authorization for Collection, Use or Disclosure of Protected Health Information

A. A carrier shall not collect, use or disclose protected health information without a valid authorization from the subject of the protected health information, except as permitted by Section 11 of this Act or as permitted or required by law or court order. Authorization for the disclosure of protected health information may be obtained for any purpose, provided that the authorization meets the requirements of this section.

B. A carrier shall retain the authorization or a copy thereof in the record of the individual who is the subject of the protected health information.

C. A valid authorization shall be in writing and contain all the following:

(1) The identity of the individual who is the subject of the protected health information;

(2) A description of the types of protected health information to be collected, used or disclosed. If the authorization is in support of an application for coverage where tests, including genetic tests, and examinations are to be performed in conjunction with underwriting the application, the authorization shall include a description of the types of tests or examinations to be performed and shall be accompanied by a statement that the tested individual may choose whether to receive the results of any laboratory tests or medical examinations performed. In cases where the authorization is other than in support of an application for coverage, and tests, including genetic tests, and examinations are to be performed, an individual may choose whether to receive the results of any laboratory tests or medical examinations performed and obtain, upon request, a detailed list of laboratory tests or medical examinations to be performed before tests or examinations are administered;

(3) A general description of the sources from which protected health information will be collected;

(4) The name and address of the person to whom the protected health information is to be disclosed, except that an authorization provided to a carrier for collection of protected health information to support insurance functions listed in Section 10H may generally describe the persons to whom protected health information may be disclosed;

(5) The purpose of the authorization, including the reason for the collection, the intended use of the protected health information, and the scope of any disclosures that may be made in carrying out the purpose for which the authorization is requested, provided those disclosures are not otherwise prohibited by law;

(6) The signature of the individual who is the subject of the protected health information or the individual who is legally empowered to grant authority and the date signed; and

(7) A statement that the individual who is the subject of the protected health information may revoke the authorization at any time, except as provided in Subsection G and subject to the rights of any person that acted in reliance on the authorization prior to revocation.

D. An authorization shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twelve (12) months, except an authorization signed for one of the following purposes:

(1) For the collection of protected health information to support insurance functions listed in Section 10H, in which event the authorization shall remain valid during the entire term of the policy or as long as necessary for the carrier to meet its obligations under the policy or as otherwise required by law;

(2) To support an application for, a reinstatement of, or a change in benefits under a life insurance policy, in which event the authorization shall expire in thirty (30) months or whenever the application is denied, whichever occurs first; or

(3) To support or facilitate ongoing management of a chronic condition or illness or rehabilitation from an injury.

E. A carrier shall obtain a separate authorization to disclose protected health information to an individual's employer, including the employer's designated risk manager, unless:

(1) The protected health information is disclosed pursuant to the employer's workers' compensation program, to the extent necessary for the performance of the employer's and carrier's rights and duties under state laws governing workers' compensation;

(2) The protected health information is disclosed pursuant to the employer's administration of a health and welfare benefit plan; or

(3) The protected health information is necessary to the administration of claims pursuant to a commercial lines policy.

F. A carrier shall obtain a separate authorization to collect, use or disclose protected health information if the purpose of the collection, use or disclosure under Subsection C(5) is for the marketing of services or goods, or for other commercial gain. The purpose of the collection, use or disclosure shall appear as a separate paragraph in bold type no smaller than twelve (12) point. The purpose shall be stated in clear and simple terms. The request for authorization shall specify that the authorization shall remain valid for no more than twelve (12) months and may be revoked at any time. The request for authorization shall state that the terms and conditions of all insurance policies will not be affected in any way by a refusal to give authorization. A separate authorization is not required if the use or disclosure is internal or to an affiliate and the only use of the information will be in connection with the marketing of an insurance product, provided the affiliate agrees not to disclose the information for any other purpose or to unaffiliated persons. With respect to insurance products, the individual shall be given an opportunity to indicate that he or she does not want protected health information used for marketing purposes and shall have given no indication that he or she does not want protected health information used for these purposes.

G. An individual who is the subject of protected health information may revoke an authorization at any time, subject to the rights of any person who acted in reliance on the authorization prior to notice of revocation. A revocation of an authorization shall be in writing, dated and signed. A revocation of an authorization shall be retained by the carrier in the record of the individual who is the subject of the protected health information. A carrier shall give prompt notice of the revocation to all persons to whom the carrier has disclosed protected health information in reliance on the initial authorization.

H. (1) A carrier that has collected protected health information pursuant to a valid authorization in accordance with this Act, may use and disclose the protected health information to a person acting on behalf of or at the direction of the carrier for the performance of the carrier's insurance functions: claims administration, claims adjustment and management, fraud investigation, underwriting, loss control, rate-making functions, reinsurance, risk management, case management, disease management, quality assessment, quality improvement, provider credentialing verification, utilization review, peer review activities, grievance procedures, and internal administration of compliance, managerial, information systems, and policyholder service functions. Additional insurance functions may be allowed with the prior approval of the commissioner.

(2) The protected health information shall not be used or disclosed for any purpose other than in the performance of the carrier's insurance functions, except as otherwise permitted in this Act.

I. An authorization to collect, use or disclose protected health information pursuant to this Act or a production of protected health information pursuant to a court order shall not be construed to constitute a waiver of any other privacy right provided to an individual who is the subject of protected health information by other federal or state laws, common law, or rules of evidence.

J. A person who receives protected health information from a carrier shall not use the protected health information for any purpose other than the lawful purpose for which it was disclosed.

K. Nothing in this Act requires a carrier to provide a benefit or commence or continue payment of a claim in the absence of protected health information to support or deny the benefit or claim.

L. A carrier that has collected protected health information prior to the effective date of this Act is not required to obtain an authorization for the information; however the information may only be used or disclosed in accordance with this Act after the effective date.

Drafting Note: States with laws addressing the electronic transmission of information may want to specifically authorize the use of electronic authorizations in this section.

Section 11. Collection, Use and Disclosure of Protected Health Information Without Authorization: Generally

A. A carrier may engage in the following activities with regard to protected health information without authorization in the following circumstances or as otherwise permitted by law:

(1) Collect protected health information from or disclose protected health information to a carrier, provided that the carrier that is receiving the information:

(a) Is investigating, evaluating, adjusting or settling a claim involving the individual who is the subject of the protected health information; or

(b) Has become or is considering becoming liable under a policy insuring the individual who is the subject of the protected health information as a result of a merger, acquisition or other assumption of such liability;

(2) Collect, use or disclose protected health information to the extent necessary to investigate, evaluate, subrogate or settle third party claims, provided that the claimant is the subject of the protected health information and the protected health information is used for no other purpose without a valid authorization or the use is otherwise permitted under federal or state law;

(3) (a) Collect, use or disclose protected health information to or from an insurance support organization provided that:

(i) The insurance support organization has in place health information policies, standards and procedures to ensure compliance with the requirements of this Act; and

(ii) The protected health information is used only to perform the insurance functions of claims settlement, detection and prevention of fraud, or detection and prevention of material misrepresentation or material nondisclosure; or

(iii) The protected health information is collected and used internally only to perform the insurance functions of ratemaking and ratemaking-related functions or regulatory or legislative cost analysis; and

(b) Additional insurance functions may be added to Subparagraphs (3)(a)(ii) and (iii) with prior approval of the commissioner;

(4) If the protected health information is necessary to provide ongoing health care treatment, and if the disclosure has not been limited or prohibited by the covered person who is the subject of the information, collect protected health information from or disclose protected health information to:

(a) A health care provider, employed by the carrier, who is furnishing health care to a covered person;

(b) A health care provider with whom the carrier contracts to provide health care services to covered persons; or

(c) A referring health care provider who continues to furnish health care to a covered person;

(5) Disclose protected health information to a person engaged in the assessment, evaluation or investigation of the quality of health care furnished by a provider pursuant to statutory or regulatory standards or pursuant to the requirements of a private or public program authorized to provide for the payment of health care;

(6) Subject to the limits of Section 14A, disclose protected health information to reveal a covered person's presence in a facility owned by the carrier and the covered person's general health condition, provided that the disclosure is limited to directory information, unless the covered person has restricted that disclosure or the disclosure is otherwise prohibited by law. For the purposes of this paragraph, directory information means information about the presence or general health condition of a particular covered person who is a patient or is receiving emergency health care in a health care facility. General health condition means the covered person's general health condition or status described as "critical," "poor," "fair," "good," "excellent," or in terms that denote similar conditions;

(7) Collect, use or disclose protected health information when the protected health information is necessary to the performance of the carrier's obligations under any workers' compensation law or contract;

(8) Collect protected health information from or disclose protected health information to a reinsurer, stop loss or excess loss carrier for the purpose of underwriting, claims adjudication and conducting claim file audits;

(9) Collect protected health information from the individual who is the subject of the protected health information; and

(10) Collect, use or disclose protected health information when the protected health information is obtained from public sources such as newspapers, public agency reports, and law enforcement or public safety reports.

B. Unless otherwise restricted by this section, a carrier that has collected protected health information without an authorization pursuant to Section 11A, may use and disclose the information to a person acting on behalf of or at the direction of the carrier to perform the insurance functions listed in Section 10H.

C. A carrier shall disclose protected health information in any of the following circumstances:

(1) To federal, state or local governmental authorities to the extent the carrier disclosing the protected health information is required by law to report protected health information or for fraud reporting purposes;

(2) The protected health information is needed for one of the following purposes:

(a) To identify a deceased individual;

(b) To determine the cause and manner of death by a chief medical examiner or the medical examiner's designee; or

(c) To provide necessary protected health information about a deceased individual who is a donor of an anatomical gift;

(3) To a state department of insurance that is performing an examination, investigation, or audit of the carrier; or

(4) Pursuant to a court order issued after the court's determination that the public interest in disclosure outweighs the individual's privacy interest and that the protected health information is not reasonably available by other means.

Drafting Note: States may wish to consider whether they should revise rules of civil procedure to establish appropriate safeguards, including notice mechanisms and protective orders, restricting redisclosure, to protect the rights of individuals who are subjects of protected health information in the context of litigation to which they are nonparties, and to avoid the misuse of subpoenas and discovery requests to circumvent the protections of this Act.

D. A disclosure of protected health information made pursuant to Subsection C shall not be construed to be or to operate as a waiver of privacy rights provided by other federal or state laws, rules of evidence or common law.

Section 12: Disclosure of Protected Health Information Without Authorization for Scientific, Medical and Public Policy Research

A. A carrier may disclose protected health information without authorization to research organizations conducting scientific, medical or public policy research as provided in this Act.

B. (1) A carrier shall keep a record of research organizations to which it discloses protected health information.

(2) The carrier shall keep the record five (5) years.

C. A carrier shall not disclose protected health information to a research organization unless the research organization agrees that the protected health information shall not be disclosed by the research organization to a third person. However, the research organization may disclose the protected health information to its agents, collaborators, or contractors as needed to conduct or assist with the research, as long as all requirements of this section are applied to the agent, collaborator, or contractor.

D. A carrier shall disclose only the minimum data necessary to conduct the intended research. Protected health information shall be disclosed only where identification is necessary to conduct the research.

E. If the scientific, medical or public policy research does not require contact with the individual who is the subject of the protected health information, the following protections shall exist prior to disclosure:

(1) The research organization develops and implements a written policy that includes procedures to assure the security and privacy of protected health information. The policy shall include:

(a) Training and disciplinary procedures to assure that persons involved in research comply with the provisions of this Act;

(b) Safeguards to assure that information in a report of the research project do not contain protected health information. The safeguards shall include a system for ensuring that only authorized individuals are able to establish a link between individuals and their health information; and

(c) A method for removing all information that identifies, directly or indirectly through reference to publicly available information, the individual who is the subject of the protected health information, when the information is no longer needed for research that is otherwise permitted under this subsection. The policy may also provide that the research organization may retain the protected health information for an indefinite period if archived in an encoded form, and it may not be used for other research unless the requirements of this section are met. "Encoded" as used in this subparagraph means that the personally identifiable information of the data is removed or encrypted and the key to restore the protected health information is retained in a secure place within the research organization with access limited to the minimum number of people necessary to maintain the confidentiality and integrity of the key.

(2) (a) The research organization prepares a research plan that explains the purposes of the research, a general description of research methods to be used, and the potential benefits of the research.

(b) (i) All research plans using protected health information under this Act shall be available to the public and may be obtained by written request to the chief executive officer of the research organization or carrier.

(ii) If the research plan contains information that is proprietary or protected from disclosure by contract or statute, the information may be deleted from the copy made available to the public.

(iii) The research organization shall keep the research plan on file for five (5) years.

(3) (a) The carrier and the research organization shall execute a written agreement:

(i) Stating the purposes of the research;

(ii) Explaining how the purposes qualify as scientific, medical or public policy research;

(iii) Documenting that the organization is qualified under Paragraphs (1) and (2) of this subsection;

(iv) Stating the expected time during which the data will be used for the stated purposes;

(v) Explaining the planned method of disposition of the protected health information at the end of the term of use; and

(vi) Stating that the written agreement shall be available to the public and can be obtained by written request to the chief executive officer of the research organization.

(b) The carrier shall provide a copy of the written, executed agreement upon request to any person. If the executed agreement contains information that is proprietary or protected from disclosure by contract or statute, the information may be deleted from the copy that is made available pursuant to this subsection.

(c) The carrier shall keep this agreement on file five (5) years.

F. If the scientific, medical or public policy research requires contact with the individual who is the subject of protected health information, the following protections shall exist prior to disclosure:

(1) The research organization and carrier shall meet the requirements of Subsection E; and

(2) (a) The research organization is responsible for obtaining a legally effective informed consent of the subject or the subject's legally authorized representative. A research organization shall seek consent only under circumstances that provide the prospective subject or the representative with sufficient opportunity to consider whether to participate in the research, and that minimize the possibility of coercion or undue influence.

(b) The information that is given to the subject or the representative shall be in language understandable to the subject or the representative.

(c) No informed consent, whether oral or written, may include any exculpatory language through which the subject or the representative waives or appears to waive any of the subject's legal rights, or releases or appears to release the investigator, the sponsor, the research organization or its agents from liability or negligence.

(d) Basic elements of informed consent. In seeking informed consent the following information shall be provided to each subject:

(i) A statement that the study involves research, an explanation of the purposes of the research and the expected duration of the subject's participation, a description of the procedures to be followed, and identification of any procedures that are experimental;

(ii) A description of any reasonably foreseeable risks or discomforts to the subject;

(iii) A description of any benefits to the subject or to others that may reasonably be expected from the research;

(iv) A disclosure of appropriate alternative procedures or courses of treatment, if any, that might be advantageous to the subject;

(v) A statement describing the extent to which confidentiality of records identifying the subject will be maintained;

(vi) For research involving more than minimal risk, an explanation as to whether any compensation and medical treatments are available if injury occurs and, if so, what they consist of, or where further information may be obtained;

(vii) An explanation of whom to contact for answers to pertinent questions about the research and the research subject's rights;

(viii) The name of a person to contact in the event of a research-related injury to the subject; and

(ix) A statement that participation is voluntary, refusal to participate will involve no penalty or loss of benefits to which the subject is otherwise entitled, and that the subject may discontinue participation at any time without penalty or loss of benefits to which the subject is otherwise entitled.

(e) Additional elements of informed consent. When appropriate, one or more of the following shall also be provided to each subject:

(i) A statement that the particular treatment or procedure may involve risks to the subject (or to the embryo or fetus, if the subject is or may become pregnant) that are currently unforeseeable;

(ii) Anticipated circumstances under which the subject's participation may be terminated by the investigator without regard to the subject's consent;

(iii) Any additional costs to the subject that may result from participation in the research;

(iv) The consequences of a subject's decision to withdraw from the research and procedures for orderly termination of participation by the subject;

(v) A statement that significant new findings developed during the course of the research that may relate to the subject's willingness to continue participation will be provided to the subject; and

(vi) The approximate number of subjects involved in the study.

(f) If a research organization submits research for approval by an institutional review board under the Federal Policy for the Protection of Human Subjects, as originally published in 56 Federal Register 28000 (1991) and as adopted and implemented by a federal department or agency, compliance with that process will be deemed compliance with the provisions of Subsections E(2) and F(2) of this section.

G. (1) If a carrier discloses to an organization conducting scientific, medical or public policy research health information that is not protected health information because all identifying information is encrypted, the carrier and research organization shall execute a written agreement that provides:

(a) That the research organization will not re-release the data accompanied by the encrypted indentifying information to a third person. However, the research organization may disclose protected health information to its agents, collaborators, or contractors as needed to conduct or assist with the research, as long as all requirements of this section are applied to the agent, collaborator, or subcontractor;

(b) That the research organization shall make no efforts to link any health information it received with encrypted indentifying information to any other data that may identify the individual who is the subject of the information; and

(c) That the research organization shall make no efforts to link any encrypted protected health information with any other identifiable data.

(2) Prior to any encrypted information being decrypted or linked to identifying data, the research organization shall comply with the requirements set forth in this section and health information with decrypted identifying information shall be deemed protected health information.

H. Nothing in this Act shall be construed to prevent the creation, use or release of anonymized data for which there is no reasonable basis to believe that the information could be used to identify an individual.

I. Nothing in this section shall be construed as superseding federal laws and regulations governing scientific, medical and public policy research.

Section 13. Unauthorized Collection, Use or Disclosure of Protected Health Information

An unauthorized collection, use, or disclosure of protected health information by a carrier is prohibited and subject to the penalties set forth in Section 15. An unauthorized collection, use or disclosure includes:

A. Unauthorized publication of protected health information;

B. Unauthorized collection, use or disclosure of protected health information for personal or professional gain, including unauthorized research that does not meet the requirements of this Act;

C. Unauthorized sale of protected health information;

D. Unauthorized manipulation of coded or encrypted health information that reveals protected health information; and

E. Use of deception, fraud, or threat to procure authorization to collect, use or disclose protected health information.

Section 14. Right to Limit Disclosures

A. A carrier shall limit disclosure of information, including health information, about an individual who is the subject of the information if the individual clearly states in writing that disclosure to specified individuals of all or part of that information could jeopardize the safety of the individual. Disclosure of information under this subsection shall be limited consistent with the individual's request, such as a request for the carrier to not release any information to a spouse to prevent domestic violence.

B. Except as otherwise required by law, a carrier shall not disclose protected health information concerning health services related to reproductive health, sexually transmitted diseases, substance abuse and behavioral health, including mailing appointment notices, calling the home to confirm appointments, or mailing a bill or explanation of benefits to a policyholder or certificateholder, if the individual who is the subject of the protected health information makes a written request. The written request shall include information as to how any amounts payable by the individual will be handled. In addition, a carrier shall not require the individual to obtain the policyholder's or certificateholder's authorization to receive health care services or to submit a claim. Except as provided in Subsection C, this section shall not apply to minors.

Drafting Note: States are reminded to ensure consistency with existing state laws addressing privacy of information related to specific health services and to amend the list of services in Subsection B accordingly.

C. (1) A carrier shall recognize the right of any minor who may obtain health care without the consent of a parent or legal guardian pursuant to state or federal law, to exclusively exercise rights granted under this Act regarding health information; and

(2) A carrier shall not disclose any protected health information related to any health care service to which the minor has lawfully consented, including mailing appointment notices, calling the home to confirm appointments, or mailing a bill or explanation of benefits to a policyholder or certificateholder, without the express authorization of the minor. In addition, a carrier shall not require the minor to obtain the policyholder's or certificateholder's authorization to receive health care services to submit a claim.

Drafting Note: The age of consent and the health care services to which a minor may consent may vary depending on state law. Health care services to which a minor may consent typically include those relating to reproductive health services, sexually transmitted disease, substance abuse and behavioral health.

Drafting Note: States should examine existing state laws and amend statutes that conflict with this section, such as laws that require the carrier to send explanations of benefits to policyholders.

E. A carrier that cannot comply with the requirements of this section relating to the suppression of benefit, payment and similar information by the effective date of this Act because of demonstrated financial or technological burdens may make a written request to the commissioner for an extension of the time permitted for compliance. The request shall propose a plan and a timetable for compliance not to exceed eighteen (18) months after the effective date of this Act. Carriers that are granted an extension by the commissioner shall report this extension and the lack of current compliance with the provisions of this section in the notice of health information policies, standards and procedures required by Section 6.

Section 15. Sanctions

Drafting Note: Insert the title of the regulatory official charged with prosecuting violations of the law on behalf of the insurance department wherever the term "commissioner" appears in this section.

A. Civil Sanctions

(1) Whenever the commissioner has reason to believe that a person has committed gross negligence in violation of a material provision of this Act and that an action under this section is in the public interest, the commissioner may bring an action to enjoin violations of this Act. An injunction issued under this section shall be issued without bond.

(2) In addition to the relief available pursuant to Paragraph (1) of this subsection, the commissioner may request and the court may order any other temporary or permanent relief as may be in the public interest, including any of the following, or any combination of the following:

(a) A civil penalty of not more than $10,000 for each violation, not to exceed $50,000 in the aggregate for multiple violations;

(b) A civil penalty of not more than $250,000 if the court finds that violations of this Act have occurred with sufficient frequency to constitute a general business practice; and

(c) Reasonable attorney fees, investigation and court costs.

Drafting Note: States should consider, consistent with existing state laws, whether they wish to allow a private right of action to individuals aggrieved by a violation of this Act.

B. Criminal Sanctions

(1) The penalties described in Paragraph (2) of this subsection shall apply to a person that collects, uses or discloses protected health information in knowing violation of this Act.

(2) A person described in Paragraph (1) shall:

(a) Be fined not more than $50,000, imprisoned not more than one year; or both;

(b) If the offense is committed under false pretenses, be fined not more than $250,000, imprisoned not more than five (5) years, or any combination of these penalties; or

(c) If the offense is committed with the intent to sell, transfer or use protected health information for malicious harm, be fined not more than $500,000, imprisoned not more than ten (10) years, or any combination of these penalties.

C. In any claim made under this section relating to an unauthorized disclosure in which a carrier is being sued under a theory of vicarious liability for the actions or omissions of the carrier's employees, it shall be an affirmative defense that the carrier substantially complied with the requirements of Section 5 of this Act.

D. An individual may not maintain an action against a carrier that disclosed protected health information in good faith reliance on the individual's authorization, if that authorization meets the requirements of Section 10 of this Act and if the disclosure was made in compliance with the requirements of this Act.

E. A person may not maintain an action against a carrier for refusing to provide information or limiting disclosure of protected health information when the refusal or limitation is based upon an individual's request pursuant to Section 14 of this Act.

Section 16. Regulations

The commissioner may, after notice and hearing, promulgate regulations to carry out the provisions of this Act. The regulations shall be subject to review in accordance with [insert statutory citation providing for administrative rulemaking and review of regulations].

Section 17. Separability

If any provision of this Act, or the application of the provision to any person or circumstance shall be held invalid, the remainder of the Act, and the application of the provision to persons or circumstances other than those to which it is held invalid, shall not be affected.

Section 18. Effective Date

This Act shall take effect on [insert a date that allows at least a one year interval between the date of enactment and the effective date.]

Chronological Summary of Action (all references are to the Proceedings of the NAIC).

1998 Proc. 2nd Quarter 11, 13-14, 752, 814-826, 829-830, 847 (adopted).