

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

SUMMARY OF PRIVACY STANDARDS

Subpart A - General Provisions

164.102 Statutory basis

Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Social Security Act and section 264 of Public Law 104-191.

164.104 Applicability Provisions of this part apply to covered entities: health plans, health care clearinghouses, and health care workers who transmit health information in electronic form in connection with any transaction referred to in section 1173(a)(1) of this subchapter.

164.106 Relationship to other parts In complying with the requirements of this part, covered entities are required to comply with the applicable provisions of parts 160 and 162 of this subchapter. **(Part 162 refers to Electronic Transactions)**

Subpart B-D [Reserved]

Subpart E Privacy of Individually Identifiable Health Information

164.500 Applicability

(1) Except as otherwise provided, the standards, requirements, and implementation specifications apply to covered entities with respect to protected health information.

(2) Health care clearinghouses (HCC) must comply as follows: (a) When a HCC creates or receives protected health information as a business associate of another covered entity the HCC must comply with: (i) Section 164.500 relating to applicability; (ii) Section 164.501 relating to definitions; (iii) Section 164.502 relating to uses and disclosures of protected health information, except that a clearing house is prohibited from using or disclosing protected health information other than is permitted in the business associate contract under which it created or received the protected health information; (iv) Section 164.504 relating to the organizational requirements for covered entities, including the designation of health care components of a covered entity; (v) Section 164.512 relating to use and disclosures for which individual authorization or an opportunity to agree or object is not required, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information; (vi) Section 164.532 relating to transition requirements and; (vii) Section 164.534 relating to compliance dates for initial implementation of the privacy standards. (b) When a HCC creates or receives protected health information other than as a business associate of a covered entity, the HCC must comply with all of the standards, requirements and implementation specifications of this subpart.

(3) The standards, requirements and implementation specifications do not apply to the Department of Defense or to any other federal agency, or non-governmental organization acting on its behalf, when providing health care to overseas foreign national beneficiaries.

164.501 Definitions Definition for *Correctional Institutions, Covered functions, Data Aggregation, Designated Record Set, Direct Treatment Relationship, Disclosure, Health Care Operations, Health Oversight Agency, Indirect Treatment Relationship, Individually Identifiable Health Information, Inmate, Law Enforcement Official, Organized Health Care Arrangement, Payment, Plan Sponsor, Psychotherapy Notes, Public Health Authority, Research, Treatment, and Use* are clearly defined.

164.502 Uses and disclosures of protected health information : general rules

IMPLEMENTATION SPECIFICATION - To comply with the standard in this Subsection, a covered entity must have Documentation of Policies and Procedures

STANDARD: Permitted Uses and Disclosures

A covered entity may not use or disclose an individual's protected health information, except to the individual (164.524 or 164.528) or for treatment, payment or healthcare operations as permitted by and in compliance with 164.506 or to the Secretary under subpart C part 160, except with respect to psychotherapy notes.

STANDARD: Minimum Necessary

A covered entity must make all reasonable efforts not to use or disclose more than the minimum amount of protected health information necessary to accomplish task. When making disclosures to public officials that are permitted under 164.514 but not required by other law, a covered entity may reasonably rely on the representations of such officials that the information requested is the minimum necessary for the task to be accomplished.

STANDARD: Uses and disclosures of PHI subject to an agreed upon restriction

A covered entity that has agreed to a restriction under 164.522 may not use or disclose the PHI covered by the restriction, except as otherwise provided in 164.522

STANDARD: Health information that meets the standard & implementation specifications for de-identification under 164.514 is considered not to be individually identifiable health information under this subpart.

STANDARD: Disclosures to Business Associates

1) A covered entity may disclose PHI to a business associate & may allow a business associate to create or receive PHI on its behalf if the entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.

2) This standard does not apply with respect to disclosures to a health care provider for treatment, health plan, health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that requirements under 164.504 are met.

STANDARD: Deceased Individuals

A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for 2 years following the death of such individual. This requirement does not apply to uses or disclosures for research purposes. See specifics relating to personal representatives, emancipated and un-emancipated minors and other implementation specifications related to this subpart.

STANDARD: Uses and Disclosures consistent with notice A covered entity that is required by 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice.

STANDARD: Confidential Communication

A covered entity must comply with the applicable requirements of 164.522(b) in communicating protected health information.

STANDARD: Disclosures by whistleblowers & workforce member crime victims

A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses PHI if they believe in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services or conditions provided by the covered entity potentially endangers one or more patients, workers or the public and the disclosure is to a health oversight agency or attorney or law enforcement official when a victim of a crime.

164.504 Uses and Disclosures: Organizational Requirements

IMPLEMENTATION SPECIFICATION - To comply with the standard in this paragraph, a covered entity must have Documentation of Policies and Procedures

Definitions for *Common Control, Common Ownership, Health Care Component and Hybrid Entity*

STANDARD: If a covered entity is a hybrid entity, the requirements of this subpart, other than the requirements of this section, apply only to the health care component(s) of the entity. In applying a provision of this subpart a reference in such provision to a covered entity refers to a health care component of the covered entity. **Safeguard Requirements:** The covered entity must ensure that a health care component of the entities complies with the applicable requirements of this subpart.

STANDARD: Business Associate contracts

A contract between a covered entity and a business associate must establish the permitted and required uses and disclosures of such information by the business associate.

164.506 Uses or disclosures to carry out treatment, payment or health care operations

IMPLEMENTATION SPECIFICATION - To comply with the standard in this paragraph, a covered entity must have Documentation of Policies and Procedures

STANDARD: Permitted uses and disclosures

Except with respect to uses or disclosures that require an authorization under 164.508, a covered entity may use or disclose protected health information for treatment, payment, or health care operations provided that such use or disclosure is consistent with other applicable requirements of this subpart. A covered entity may use or disclose protected health information for its own treatment, payment or health care operation, treatment and payment activities of another health care provider, and health care operation if each entity has or has had a relationship with the individual. A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to another covered entity that participates in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

164.508 Uses and disclosures for which an authorization is required.

IMPLEMENTATION SPECIFICATION - To comply with the standard in this paragraph, a covered entity must have Documentation of Policies and Procedures that include the requirements of a valid authorization.

STANDARD - Authorization for uses and disclosures is required for the following:

1) a) Psychotherapy notes other than the transition provisions in 164.532; b) Research that includes treatment of the individual; c) Marketing - other than the transition provisions in 164.532 a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of face-to-face communication, a promotional gift of nominal value provided by the covered entity. If remuneration, direct or indirect to the covered entity from a third party, the authorization must state the fact; and d) See this subsection for applicable restrictions and exceptions.

2) For a marketing communication to qualify under the above standard the following conditions must be met: a) Identify the covered entity as the party making the communication; b) Prominently state the fact that the covered entity has received or will receive direct or indirect remuneration for making the communication; and c) If the communication is contained in a newsletter or similar type of general

communication device to a broad cross section of patients, enrollees it must contain instructions describing how the individual may opt out of receiving future such communications.

164.510 Uses and Disclosures requiring an opportunity for the individual to agree or to object

A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree or prohibit or restrict the use or disclosure, in accordance with this section

IMPLEMENTATION SPECIFICATION - To comply with the standard in this paragraph, a covered entity must have Documentation of Policies and Procedures

STANDARD - Use and disclosure for facility directories

1) Permitted uses and disclosures - Except when an objection is expressed in accordance with paragraphs below a covered health care provider may: a) Use the following protected health information to maintain a directory of individuals in its facility: Name, location in the facility, condition described in general terms that does not communicate specific medical information; religious affiliation; b) Disclose for directory purposes such information to: members of the clergy; or c) Except religious affiliation, to other persons who ask for the individual by name.

2) Opportunity to object: A provider must inform an individual of the information that it may include in a directory and the persons to whom it may disclose such information and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted.

3) Emergency circumstances: If due to an emergency situation, the opportunity to object cannot practically be provided a provider may use or disclose some or all of the information permitted for the directory if: a) Disclosure is consistent with a prior expressed preference of the individual if any is known b) Disclosure is in the individual's best interest as determined by the provider, in the exercise of professional judgment

STANDARD - Use and disclosure for involvement in the individual's care and notification purposes

1) Permitted uses and disclosures: a) A provider may disclose to a family member, other relative or a close personal friend of the individual, or any other person identified by the individual, information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care; and b) A provider may use or disclose information to notify or assist in the notification of (including identifying or locating) a family member, a personal representative of the individual or another person responsible for the care of the individual of the individual's location, general condition or death.

2) With the individual present and has the capacity to make health care decisions, the provider may use or disclose information if it: a) Obtains the individual's agreement; b) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or c) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

3) Limited uses and disclosures when the individual is not present or disclosure cannot be practically provided due to incapacity or an emergency situation: a) The provider may in the exercise of professional judgment determine whether the disclosure is in the best interest of the individual and disclose only the information that is directly relevant to the person's involvement with the individual's health care. (i) Such as allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

4) Use and disclosures for disaster relief purposes: A provider may use or disclose information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts for the purpose of coordinating with such entities the above paragraphs.

164.512 Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required

IMPLEMENTATION SPECIFICATION - To comply with the standard in this paragraph, a covered entity must have Documentation of Policies and Procedures

A covered entity may use or disclose protected health information without the written authorization of the individual as described in 164.508 or the opportunity for the individual to agree or object as described in 164.510 in the situations covered by this section.

STANDARD: Permitted uses and disclosure for public health activities

A covered entity may disclose protected health information for activities and purposes of:

- 1) Public health activities including disease, reporting, child abuse, neglect, domestic violence, workplace surveillance for work related illness or injury
- 2) Health oversight activities including audits, civil, administrative or criminal investigations, licensure, inspections, or disciplinary actions
- 3) Judicial and administrative proceedings in response to an order of a court or administrative tribunal; in response to a subpoena, discovery request or other lawful process
- 4) Law enforcement purposes with and as limited by the relevant requirements of a court order, warrant, subpoena or summons, a grand jury subpoena
- 5) Information for identification and location purposes is limited to name and address; date and place of birth; social security number; ABO blood type and rH factor; type of injury; date and time of treatment; date and time of death; description of physical characteristics; with exceptions of DNA, dental records, typing samples or analysis of body fluids or tissue unless requested with legal document requests or the individual agrees to the disclosure

- 6) Victims of crime may agree to the disclosure, the law enforcement official represents that such information is needed to determine whether a violation of the law has occurred and information is not to be used against the victim
- 7) Decedents - disclosure is permitted to coroners and medical examiners, funeral directors, for cadaver organ, eye or tissue donation purposes as necessary to carry out their duties with respect to the decedent
- 8) Research purposes requires waivers of authorization approved by IRB or a privacy board and documentation is provided within the guidelines of this subsection
- 9) Military and veterans activities, armed forces personnel, national security and intelligence activities, protective services for the president and others and medical suitability determinations proper protocol and appropriate documentation is required from the requesting source
- 10) Correctional institutions and other custodial situations for the provision of health care, health and safety. No application after release
- 11) Workers compensation authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work related injuries or illness without regard to fault
- 12) FDA jurisdiction with respect to an FDA-regulated product or activity for the purpose of activities related to the quality, safety or effectiveness of such product or activity to collect or report adverse events, product defects or problems; to track FDA-regulated products; to enable recalls, repairs or replacements or look back including locating and notifying individuals; to conduct post marketing surveillance.

164.514 Other requirements relating to uses and disclosures of protected health information

IMPLEMENTATION SPECIFICATION To comply with this subsection the covered entity must have a person with appropriate knowledge, experience, principles and methods for rendering information not individually identifiable; risk is very small that the information could be used alone or in combination with other available information to identify an individual; documents the methods and results.

STANDARD: De-identification of protected health information

Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

- 1) LIMITED DATA SETS The following identifiers are removed; names, addresses and other geographic identifiers, relatives, employers or household members; zip codes with 20,000 or fewer people the initial 3 digits is changed to 000; all elements of dates except years related to an individual; numbers including telephone, fax, ssn, medical records, beneficiary numbers, account numbers, certificate/license numbers, vin numbers, license plate numbers, device identifiers and serial numbers, URLs, IP address, biometric identifiers, photographic images and any other unique identifying number, characteristic or code.
- 2) A Data Use Agreement is required when a limited data set is used meeting the requirements of this section.

IMPLEMENTATION SPECIFICATION To comply with this subsection the covered entity must assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity

STANDARD: Re-identification

- 1) The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and
- 2) The covered entity does not use or disclose the code or other means of record identification for any other purpose and does not disclose the method for re-identification.

IMPLEMENTATION SPECIFICATION To comply with this subsection the covered entity must identify 1) Those persons or class of persons in its workforce who need access to protected health information to carry out their duties; 2) For each person or classes or persons the category or categories of protected health information to which access is needed and any conditions appropriate to such access; and 3) Must make reasonable efforts to limit the access of such persons or classes within this subsection.

IMPLEMENTATION SPECIFICATION: Minimum Necessary Disclosures Of Protected Health Information:

To comply with this subsection the covered entity must implement policies and procedures (which may be standard protocol) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. For all other disclosures, a covered entity must

- 1) Develop criteria designed to limit the health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is made.
- 2) Review requests for disclosure on an individual basis in accordance with such criteria. A covered entity may rely on a requested disclosure as the minimum necessary for the stated purpose when making disclosures to public officials; another covered entity; is requested by a professional who is a member of its workforces or is a business associate for the purpose of providing professional services to the covered entity. Documentation or representations that comply with 164.512 have been provided by a person requesting the information for research purposes.

IMPLEMENTATION SPECIFICATION: Other Content Requirement

A covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose.

1) If the covered entity uses or discloses protected health information to target the communication to individuals based on their health status or conditions it must: a) Make a determination prior to making the communication that the product or service being marketed may be beneficial to the health of the type or class of individual targeted; and b) Must explain why the individual has been targeted and how the product or service relates to the health of the individual.

2) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future marketing communications are not sent such communications.

IMPLEMENTATION SPECIFICATION: Fundraising Requirements

The covered entity may not use or disclose protected health information for fundraising purposes unless a statement required by 164.520 is included in the covered entity's notice: 1) A description of how the individual may opt out of receiving any further fundraising communications; 2) The covered entity must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.

STANDARD - Uses and Disclosures of protected health information for underwriting and related purposes

If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such information for any other purpose except as may be required by law.

STANDARD - Verification Requirements

Except with respect to disclosures under 164.510 a covered entity must 1) Verify the identity of a person requesting protected health information and the authority of any such person to have access to the information if such person is not known to the covered entity; 2) Obtain any documentation, statements, representations whether oral or written from the person requesting the protected health information as required as a condition of disclosure.

The verification requirements are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with 164.510 or acts on a good faith belief in making the disclosure in accordance with 164.512(j).

164.520 Notice of privacy practices for protected health information

STANDARD: Notice of privacy practices

1) **Right to Notice:** An individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information. a) A covered entity must provide a notice no later than the date of the first service delivery, including service delivered electronically after the compliance date; in an emergency treatment situation, as soon as reasonably practicable; except in an emergency situation make a good faith effort to obtain a written acknowledgment of the receipt of notice; and b) Specific requirements for electronic notice apply as above in 1) a).

2) **Exception for group health plans:** An individual enrolled in a group health plan has a right to notice: a) From the group health plan, if such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer of HMO; or b) From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under this group health plan.

A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO and that creates or receives protected health information in addition to summary health information as defined in 164.504 or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must: a) Maintain a notice under this section; and b) Provide such notice upon request to any person except for the above health plans.

A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO and does not create or receive protected health information in addition to summary health information as defined in 164.504 or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan is not required to maintain or provide a notice under this section.

3) **Exception for inmates** An inmate does not have a right to notice under this section and the requirements of this section do not apply to a correctional institution that is a covered entity.

IMPLEMENTATION SPECIFICATION Content of Notice

1) Required elements. The covered entity must provide a notice that is written in plain language and that contains these elements: a) **Header**. The notice must contain the following statement as a header or otherwise prominently displayed:

" THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY"

b) **Uses and Disclosures** (1) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment and health care operations; (2) A description of each of the other purposes for which the covered entity is permitted or required to use or disclose information without the individual's written consent or authorization; (3) If a use or disclosure for any purpose described in these

paragraphs is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law; (4) The description must include sufficient detail to plan the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law; and (5) A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization.

c) Separate Statements for certain uses and disclosures

A separate statement for the engagement in any of the following activities is required: (1) The covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health related benefits and services that may be of interest to the individual; (2) The covered entity may contact the individual to raise funds for the covered entity; and (3) A group health plan, or a health plan insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.

d) Individual rights: The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights as follows: (1) The right to request restrictions on certain uses and disclosures and that the covered entity is not required to agree to a requested restriction; (2) The right to receive confidential communications of protected health information as applicable; (3) The right to inspect and copy protected health information; (4) The right to amend protected health information.; (5) The right to receive an accounting of disclosures of protected health information; and (6) The right of an individual, including an individual who has agreed to receive the notice electronically to obtain a paper copy of the notice from the covered entity upon request.

e) Covered entities duties: (1) The notice must contain a statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information; (2) A statement that the covered entity is required to abide by the terms of the notice currently in effect; and (3) A statement that it reserves the right to change the terms of the notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.

f) Complaints: The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity and a statement that the individual will not be retaliated against for a filing a complaint.

g) Contact: The notice must contain the name, the title, and telephone number of a person or office to contact for further information.

h) Effective Date: The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

2) Optional Elements: A covered entity may elect to limit the uses and disclosures, describe those limits provided that they do not include a limit that is required by law or permitted under other sections.

3) Revisions to the Notice: Whenever there is a material change the covered entity must promptly revise and distribute the notice. Except when required by law, a material change may not be implemented prior to the effective date of the notice in which such material change is reflected.

IMPLEMENTATION SPECIFICATION Provision of notice

A covered entity must make the notice required by this section available on request to any person and to individuals as specified.

1) Specific requirements for health plans: (a) A health plan must provide notice no later than the compliance date for the health plan to individuals then covered by the plan; (b) Thereafter, at the time of enrollment to individuals who are new enrollees; (c) Within 60 days of a material revision to the notice, to individuals then covered by the plan; (d) No less frequently than once every three years the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice; (e) The health plan satisfies the requirements if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents; (f) If a health plan has more than one notice it satisfies the requirements by providing the notice that is relevant to the individual or other person requesting the notice.

2) Specific requirements for certain covered health care providers: A covered health care provider that has direct treatment relationship with an individual must: (a) Provide the notice no later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; (b) If the covered health care provider maintains a physical service delivery site they must have the notice available at the delivery site for individuals to request to take with them and whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements.

3) Specific requirements for electronic notice: (a) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site; (b) A covered entity may provide the notice required to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered

entity will satisfy the provision requirements when timely; (c) If the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service; and (d) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

IMPLEMENTATION SPECIFICATION Joint notice by separate covered entities.

Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that a) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice as part of its participation in the organized health care arrangement; b) The joint notice meets the implementation specifications except for the fact that the statements required may be altered to reflect the fact that the notice covers more than one covered entity and describes with reasonable specificity the covered entities or class of entities to which the joint notice applies, the service delivery sites or classes of service delivery sites; c) If applicable, the notice states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment or health care operations relating to the organized health care arrangement; d) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications; and e) Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of this section with respect to all others covered by the joint notice.

IMPLEMENTATION SPECIFICATION Documentation

A covered entity must document compliance with the notice requirements by retaining copies of the notices issued by the covered entity for a period of 6 years from the date of its creation or the date when it was last in effect, whichever is later (164.530(j)).

164.522 Rights to request privacy protection for protected health information

STANDARD: Right of an individual to request restriction of uses and disclosures

- 1) A covered entity must permit an individual to request that the covered entity restrict: a) Uses or disclosures of information about the individual to carry out treatment, payment or health care operations; and b) Disclosures permitted under 164.510(b)
- 2) A covered entity is not required to agree to a restriction.
- 3) A covered entity who agrees to a restriction may not use or disclose information in violation of the restriction, except when the individual is in need of emergency treatment and the restricted information is needed to provide that emergency treatment.
- 4) If restricted information is disclosed to a health care provider for emergency treatment, the covered entity must request that the provider not further use or disclose the information.
- 5) A restriction agreed to by a covered entity is not effective under this subpart to prevent uses or disclosures under 164.502(a)(2)(ii), 164.510(a) or 164.512.

STANDARD: Terminating a restriction

A covered entity may terminate its agreement to a restriction if: a) The individual agrees to or requests the termination in writing; b) The individual orally agrees to the termination and the oral agreement is documented; or c) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to information created or received after it has so informed the individual.

IMPLEMENTATION SPECIFICATION Documentation

A covered entity that agrees to a restriction must document the restriction in accordance with policy and procedures developed under 164.530 Administrative Requirements and this documentation must be maintained and retained accordingly.

STANDARD: Confidential communications requirements

- 1) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.
- 2) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

IMPLEMENTATION SPECIFICATION Conditions on providing confidential communications.

- 1) A covered entity may require the individual to make a request for a confidential communication in writing.
- 2) A covered entity may condition the provision of a reasonable accommodation on a) When appropriate, information as to how payment, if any, will be handled; and b) Specification of an alternative address or other method of contact
- 3) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communication on a confidential basis.
- 4) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

164.524 Access of individuals to protected health information

STANDARD - Access to protected health information

1) **Right of access** - except as otherwise stated, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for: a) Psychotherapy notes; b) Information compiled in reasonable anticipation of, or for use in, a civil, criminal or administration action or proceeding; and c) Protected health information maintained by a covered entity that is: (1) Subject to the CLIA of 1988 to the extent the provision of access to the individual would be prohibited by law; or (2) Exempt from the CLIA of 1988.

2) **Unreviewable grounds for denial** - A covered entity may deny an individual access without providing the individual an opportunity for review in the following circumstances: a) The information is excepted from the right of access by the above paragraphs; b) A covered entity that is a correctional institution or a covered health provider acting under the direction of a correctional institution may deny, in whole or in part, an inmate's request if obtaining such copy would jeopardize the health, safety, security, custody or rehabilitation of the individual or of other inmates, officers, employees or other persons associated with the institution; c) An individual's access to information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment and the covered health care provider; d) An individual's access to information that is contained in records that are subject to the Privacy Act, 5 U.S.C 552a, may be denied, if the denial of access under the Act would meet the requirements of the law; e) An individual's access may be denied if the information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

3) **Reviewable grounds for denial** - A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required in above paragraphs in the following circumstances: a) A licensed health care professional has determined, in the exercise of good judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; b) The information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or c) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to another person.

4) **Review of a denial of access** - If access is denied on a ground permitted in the above paragraph, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under subsequent paragraphs.

IMPLEMENTATION SPECIFICATION: Requests for access and timely action

1) The covered entity must permit an individual to request access to inspect or to obtain a copy of the information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

2) The covered entity must act on the request for access no later than 30 days after receipt of the request as follows: a) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with subsequent paragraphs; b) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with subsequent paragraphs; c) If the request for access is for information that is not maintained or accessible to the covered entity on-site, the covered entity must take an action no later than 60 days from the receipt of such a request; d) If the covered entity is unable to take an action with the time required, the covered entity may extend the time for such actions no more than 30 days provided a written statement is sent to the individual with the reasons for the delay and the date by which the covered entity will complete its action on the request and there may be only one such extension.

IMPLEMENTATION SPECIFICATION: Provision of access

1) The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the information is maintained in more than one record set or in more than one location, the covered entity need only produce the information once in response to a request for access.

2) The covered entity must provide the individual with access to the information in the form or format requested by the individual, if it is readily producible in such form or format; if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual.

- 3) The covered entity may provide the individual with a summary of the information requested in lieu of providing access to the information or may provide an explanation of the information to which access has been provided if the individual agrees in advance to such a summary or explanation and the individual.
- 4) The covered entity must provide the access as requested by the individual in a timely manner, including arranging with the individual for a convenient time and place to inspect or obtain a copy or mailing the copy of the information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request with the individual as necessary to facilitate the timely provision of access.
- 5) If the individual requests a copy of the information or agrees to a summary or an explanation the covered entity may impose a reasonable, cost-based fee provided the fee includes only the cost of copying (including supplies and labor), postage (when the copy must be mailed) and preparing an explanation or summary if agreed to by the individual in advance.

IMPLEMENTATION SPECIFICATION: Denial of access

- 1) If the covered entity denies access, in whole or in part, to information, the entity must comply with the following requirements: a) The covered entity must to the extent possible, give the individual access to any other information requested, after excluding the information as to which the entity has a ground to deny access.
- 2) The covered entity must provide a timely, written denial to the individual in accordance with this section. The denial must be in plain English and contain: a) The basis for the denial b) A statement of the individual's review rights under this section including a description of how the individual may exercise such review rights. c) A description of how the individual may complain to the entity pursuant to the complaint procedures under 164.530(d) or to the Secretary pursuant to the procedures in 160.306. The description must include the name, or title and telephone number of the contact person or office designated in 164.530.
- 3) If the covered entity does not maintain the information and knows where the information is maintained, the covered entity must inform the individual where to direct the request for access.
- 4) If the individual has requested a review of a denial, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards above. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

IMPLEMENTATION SPECIFICATION: Documentation

A covered entity must document the following and retain the documentation as required by 164.530: 1) The designated record sets that are subject to access by individuals 2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

164.526 Amendment of protected health information

STANDARD: Right to amend

- 1) An individual has the right to have a covered entity that is a health care provider amend protected health information about him or her in designated record sets of the covered entity for as long as the covered entity maintains the information.
- 2) A covered entity may deny a request for amendment or correction under certain circumstances: a) Was not created by the covered entity unless the individual provides a reasonable basis to believe that the originator is no longer available to act on the requested amendment; b) It is not part of the designated record set; c) Would not be available for inspection under 164.524; or d) Is accurate and complete.

IMPLEMENTATION SPECIFICATION - Requests for amendment and timely action.

- 1) The covered entity must permit an individual to request that the covered entity amend the information maintained in a designated record set. The covered entity may require individuals to make requests in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.
- 2) The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows: a) If the covered entity grants the requested amendment, it must take the actions required by the above sections; and b) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with this section.
- 3) If the covered entity is unable to act on the amendment with the time required, the covered entity may extend the time for such actions no more than 30 days provided a written statement is sent to the individual with the reasons for the delay and the date by which the covered entity will complete its action on the request and there may be only one such extension.

IMPLEMENTATION SPECIFICATION - Accepting the amendment

If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements: a) The covered entity must make the appropriate amendment to the information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment; b) The covered entity must timely inform the individual that the

amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with above section; c) The covered entity must make reasonable efforts to inform and provide the amendment with in a reasonable time to persons identified by the individual as needing the amendment, including business associates that the covered entity knows have the information needing the amendment.

IMPLEMENTATION SPECIFICATION - Denying the amendment

- 1) The covered entity must provide an individual with a timely, written denial in accordance with the above sections. The denial must use plain language and contain: a) The basis for the denial; b) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement; c) A statement that if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the information that is subject to the amendment; and d) A description of how the individual may complain to the entity pursuant to the complaint procedures under 164.530(d) or to the Secretary pursuant to the procedures in 160.306. The description must include the name, or title and telephone number of the contact person or office designated in 164.530.
- 2) The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial or all or part of a requested amendment and that basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.
- 3) The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.
- 4) The covered entity must, as appropriate, identify the record or information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any and the covered entity's rebuttal, if any to the record set.
- 5) If a statement of disagreement has been submitted by an individual, the covered entity must include the material appended in accordance with above paragraphs or at the election of the covered entity, an accurate summary of any such information with any subsequent disclosure of the information to which the disagreement relates.
- 6) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial or an accurate summary of such information, with any subsequent disclosure of the information only if the individual has requested such action.
- 7) When a subsequent disclosure is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by above paragraph as applicable to the recipient of the standard transaction.

IMPLEMENTATION SPECIFICATION - Actions on notices of amendment

A covered entity that is informed by another covered entity or an amendment to an individual's information must amend the information in designated record sets.

IMPLEMENTATION SPECIFICATION - Documentation

A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by 164.530(j) (for a period of six years).

164.528 Accounting of disclosures of protected health information

STANDARD: Right to an accounting of disclosures of protected health information

- 1) An individual has a right to receive an accounting of all disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures a) To carry out treatment, payment and healthcare operations; b) To individual's of information about them as provided in 164.506; c) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in 164.510; d) For national security or intelligence purposes as provided in 164.512; e) To correctional institutions, law enforcement officials as provided in 164.512; f) That occurred prior to the compliance date for the covered entity; and g) As part of a limited data set in accordance with 164.514.
- 2) A covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that the accounting would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required; a) If the statement is made orally the covered entity must document the statement including the identity of the agency or official making the statement; b) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; c) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.
- 3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

IMPLEMENTATION SPECIFICATION - Content of the accounting

The covered entity must provide the individual with a written accounting meeting the following requirements:

- 1) The accounting must include disclosures of information that occurred during the six years (or such shorter time period as the request of the individual) prior to the date of the request including disclosures to or by business associates of the covered entity.
- 2) The accounting must include for each disclosure: (a) The date of the disclosure; (b) The name of the entity or person who received the protected health information and if known the address of such entity or person; (c) A brief description of the protected health information disclosed; (d) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement a copy a written request for a disclosure.
- 3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose or pursuant to a single authorization the accounting may with respect to such multiple disclosures: (a) provide the information required for the first disclosure during the accounting period; (b) provide the frequency, periodicity or number of disclosures made during the accounting period and; (c) provide the date of the last such disclosure during the accounting period.
- 4) If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in accordance with 164.512 for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included; (a) provide the name of the protocol or other research activity (b) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records; (c) A brief description of the type of protected health information that was disclosed; (d) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure; (e) The name, address and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; (f) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity; and (g) At the request of the individual the covered entity shall assist in contacting the entity that sponsored the research and the researcher.

IMPLEMENTATION SPECIFICATION - Provision of the accounting

- 1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request as follows: a) The covered entity must provide the individual with the accounting requested; b) If the covered entity is unable to provide the accounting within the time required the covered entity may extend the time to provide the accounting by no more than 30 days, provided the covered entity provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting and the covered entity may have only one such extension.
- 2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent accounting by the same individual within the same 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

IMPLEMENTATION SPECIFICATION - Documentation

- 1) A covered entity must document the following and retain the documentation in writing or electronically for a period of six years from the date of its creation or the date when it last was in effect, whichever is later: a) The information required to be included in the above paragraph; b) The written accounting that is provided to the individual under this section; c) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

164.530 Administrative requirements

STANDARD Personnel designations

- 1) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.
- 2) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by 164.520.

IMPLEMENTATION SPECIFICATION - Personnel designations

- 1) A covered entity must document the personnel designations according to the standards of this subparagraph.

STANDARD: Training

- 1) A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.

IMPLEMENTATION SPECIFICATION - Training

- 1) A covered entity must provide training that meets the requirements as follows: a) To each member of the covered entity's workforce by no later than the compliance date for the covered entity; b) Thereafter,

to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and c) To each member of the covered entity's workforce whose functions are affected by a material change in the policies and procedures required by this subpart, within a reasonable period of time after the material change becomes effective.

2) A covered entity must document that the training has been provided for each member of the workforce.

STANDARD: Safeguards

1) A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

IMPLEMENTATION SPECIFICATION - Safeguards

A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

STANDARD: Complaints to the covered entity

A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart or its compliance with such policies and procedures or the requirements of this subpart.

IMPLEMENTATION SPECIFICATION - Documentation of complaints

A covered entity must document all complaints received and their disposition, if any.

STANDARD: Sanctions

A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of 164.502(j) or under subsequent subparagraphs of this subpart.

IMPLEMENTATION SPECIFICATION - Documentation

A covered entity must document the sanctions that are applied, if any.

STANDARD: Mitigation

A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use of disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

STANDARD: Refraining from intimidating or retaliatory acts

A covered entity may not intimidate, threaten or coerce, discriminate against or take other retaliatory action against: a) Any individual for the exercise by the individual of any right under, or for the participation by the individual in any process established by this subpart, including the filing of a complaint under this section b) Any individual or other person for filing of a complaint with the Secretary, testifying or assisting or participating in an investigation, compliance review, proceeding or hearing; opposing any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.

STANDARD: Waiver of rights

A covered entity may not require individuals to waive their rights under 160.306 as a condition of the provision of treatment, payment, enrollment in a health plan or eligibility of benefits.

STANDARD: Policies and Procedures

A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification or other requirement.

STANDARD: Changes to policies or procedures

1) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications.

2) When a covered entity changes a privacy practice that is stated in the notice and makes corresponding changes to policies and procedures, it may make the changes effective for information that it created or received prior to the effective date of the notice revision if the covered entity included in the notice a statement reserving its right to make such a change in its privacy practice or a covered entity may make changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with this subpart.

IMPLEMENTATION SPECIFICATION - Changes in law

Whenever there is a change in law that necessitates a change to the covered entity's policies and procedures the covered entity must promptly document and implement the revised policies and procedures. If the change in the law materially affects the content of the notice, the covered entity must promptly make the appropriate revisions to the notice. Nothing may be used by a covered entity to excuse a failure to comply with the law.

IMPLEMENTATION SPECIFICATION - Changes to privacy practices stated in the notice. 1) To implement a

change stated in the notice a covered entity must a) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice complies with this subpart.

b) Document the policy or procedure as revised c) Revise the notice as required. The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice. 2) If a covered entity has not reserved its right to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practice as stated in the notice. A covered entity may change a privacy practice that is stated in the notice and the related policies and procedures without having reserved the right to do so, provided a) Such change meets the implementation requirements of this subpart. b) Such change is effective only with respect to protected health information created or received after the effective date of the notice.

IMPLEMENTATION SPECIFICATION - Changes to other policies and procedures

A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice provided: a) The policy or procedure, as revised, complies with all standards, requirements, implementation specification of this subpart; and b) Prior to the effective date of the change, the policy or procedure as revised is documented as required by this section

STANDARD: Documentation

A covered entity must: a) Maintain the policies and procedures provided for in this section in written or electronic form; b) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and c) If an action or activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity or designation.

IMPLEMENTATION SPECIFICATION - Retention Period

A covered entity must retain the documentation required by this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

STANDARD: Group Health Plans

A group health plan is not subject to the standards or implementation specifications in the above paragraphs with the exception of refraining from intimidation or retaliatory actions, waiver of rights and documentation to the extent that: 1) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; 2) The group health plan does not create or receive protected health information except for summary health information or information on whether the individual is participating in the group health plan or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan; and 3) A group health plan is subject to the standard and implementation specification in this section only with respect to plan documents amended in accordance with 164.504.

164.532 Transition provisions

STANDARD: Effect of prior consents

Notwithstanding other sections of this subpart, a covered entity may use or disclose PHI pursuant to an authorization, or other express legal permission obtained from an individual permitting the use and disclosure of PHI, informed consent of the individual to participate in research, or a waiver of informed consent by an IRB.

IMPLEMENTATION SPECIFICATION - Effect of prior authorization for purposes other than research. 1) If the authorization, or other express legal permission obtained permits a use or disclosure for purposes of carrying out treatment, payment or health care operations, the covered entity may, with respect to PHI that it created or received before the applicable compliance date and to which the authorization or other express legal permission obtained applies, use or disclose such information, provided that: a) The covered entity does not make any use or disclosure that is expressly included from the authorization, or other express legal permission obtained. b) The covered entity complies with all limitations placed by the authorization, or other express legal permission obtained. 2) If the authorization, or other express legal permission obtained permits a use or disclosure for a purpose other than to carry out treatment, payment or health care operations, the covered entity may, with respect to PHI that it created or received before the applicable compliance date and to which the authorization or other express legal permission obtained applies, use or disclose such information, provided that: a) The covered entity does not make any use or disclosure that is expressly included from the authorization, or other express legal permission obtained. b) The covered entity complies with all limitations placed by the authorization, or other express legal permission obtained.

IMPLEMENTATION SPECIFICATION - Effect of prior permission for research.

If the authorization, or other express legal permission obtained permits a use or disclosure for purposes of research the covered entity may, with respect to PHI that it created or received before the applicable compliance date and to which the authorization or other express legal permission obtained applies, use or disclose such information, provided that: a) An authorization or other express legal permission from an individual to use or disclose protected health information for the research; b) The informed consent of the individual to participate in the research; and c) A waiver, by an IRB, of informed consent for the research provided that a covered entity must obtain authorization in accordance with 164.508 if, after the compliance date, informed consent is sought from an individual participating in the research.

STANDARD: Effect of prior contracts or other arrangements with business associates

A covered entity, other than a small health plan, may disclose protected health information to a business associate and may allow a business associate to create, receive or use protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does

not comply with 164.502 and 164.504 consistent with the requirements and only for such time set forth as:

IMPLEMENTATION SPECIFICATION - Deemed compliance

1) Qualification - A covered entity, other than a small health plan, is deemed to be in compliance with the documentation and contract requirements if: a) Prior to Oct 15, 2002 such covered entity has entered into and is operating pursuant to a written contract or other written arrangement with a business associate for such business associate to perform functions or activities or provide services that make the entity a business associate; b) The contract or other arrangement is not renewed or modified from Oct 15, 2002 until the compliance date of April 14, 2003.

2) Limited deemed compliance period - A prior contract or other arrangement that meets the qualification requirements of this section, shall be deemed compliant until the earlier of: a) The date such contract or other arrangement is renewed or modified on or after the compliance date of April 14, 2003 or April 14, 2004 for a small health plan.

3) Covered entity responsibilities - Nothing in this section shall alter the requirements of a covered entity to comply with part 160, subpart C of this subchapter and 164.524, 164.526, 164.528 and 164.530 with respect to protected health information held by a business associate.

164.534 Compliance dates for initial implementation of the privacy standard

1) Health care providers - A covered health care provider must comply with the applicable requirements of this subpart no later than April 14, 2003

2) Health plans - A health plan must comply with the applicable requirements of this subpart no later than the following date, as applicable: a) Health plans other than small health plans - April 14, 2003; b) Small health plans - April 14, 2004

3) Health care clearinghouses. A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 14, 2003.