HIPAA Privacy Rule Checklists
Section 164.530 – Administrative Requirements

Prepared by the
NCHICA Consent and Patients Rights Work Group
Privacy and Confidentiality Focus Group

Approved for Public Distribution
March 29, 2002

HIPAA Privacy Rule Checklists
Section 164.530 – Administrative Requirements

I. Personnel Designations

a. **Designation**. A covered entity must designate, and document the designation of, the following:

i. ____ A privacy official who is responsible for the development and implementation of the policies and procedures of the entity; *and*

ii. ____ A contact person or office who is responsible for receiving complaints under this section, and who is able to provide further information about the Privacy Notice requirements.

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

i. ____ The training provided must satisfy the following requirements:

____ The training is provided to each member of the covered entity's workforce by no later than the compliance date for the covered entity;

____ Thereafter, the training is provided to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; *and*

____ The training is provided to each member of the covered entity's workforce whose functions are affected by a material change in the Section's policies or procedures, within a reasonable period of time after the material change becomes effective.

ii. ____ A covered entity must document that the training as been provided.

II. Other Requirements

a. **Safeguards**. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications, or other requirements of this Section.

b. **Complaints**. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures, or its compliance with such policies and procedures.

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

c. **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 Section. *Note*: This standard does not apply to a member of the covered entity's workforce with respect to whistleblower-type actions that are covered elsewhere by the Rule.

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

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

e. **Refrain**. A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

i. ____ Any individual for their exercise of any right, including the filing of a complaint;

ii. ____ Any individual or other person for:

____ Filing a complaint with the Secretary;

____ Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI.

____ Opposing any act or practice made unlawful by this section, 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 section.

f. **Waiver of Rights**. A covered entity may not require individuals to waive their rights under § 160.306 or § 164.530 as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

g. **Policies and Procedures**.

i. ____ **Implementation**. 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 of this section.

____ 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 compliance.

____ This standard shall not be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this section.

ii. ____ **Changes**. A covered entity may change its policies and procedures in compliance with one of the following:

____ 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 of this section;

____ When a covered entity changes a privacy practice that is included in the Notice, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision if it has included in the Notice a statement reserving its right to make such a change in its privacy practices; *or*

____ A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with this section.

iii. ____ **Changes in Law**. Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure.

____ If the change in law materially affects the content of the Privacy Notice, the covered entity must promptly make the appropriate revisions to the Notice.

____ Nothing in this provision may be used by a covered entity to excuse a failure to comply with the law.

iv. ____ **Changes to Privacy Practices**.

____ If a covered entity has not reserved its right to change a practice that is stated in the Notice, the covered entity is bound by the privacy practices stated in the Notice with respect to protected health information created or received while the Notice is in effect.

____ 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, **if**:

____ Such change meets the implementation requirements in this section; *and*

____ Such change is effective only with respect to protected health information created or received after the effective date of the Notice.

____ To implement a change (as provided above), a covered entity must:

____ 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 the applicable standards, requirements, and implementation specifications;

____ Document the policy or procedure, as revised; *and*

____ Revise the notice as required to state the changed practice and make the revised notice available as required. *Note*: The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised Notice.

____ A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the Notice, provided that:

____ The policy or procedure, as revised, complies with the applicable standards, requirements, and implementation specifications; *and*

____ Prior to the effective date of the change, the policy or procedure, as revised, is documented (as required).

h. **Documentation**. A covered entity must:

i. ____ Maintain the policies and procedures in written or electronic form;

ii. ____ If a communication is required to be in writing, maintain such writing, or an electronic copy, as documentation; *and*

iii. ____ If an action, activity, or designation is required to be documented, maintain a written or electronic record of such action, activity, or designation.

iv. ____ Retain the documentation for six years from the date of its creation or the date when it last was in effect, whichever is later.

i. **Group Health Plans**. A group health plan is:

i. ____ Not subject to the standards or implementation specifications of this Section (except those prohibiting intimidation, the forced waiver of rights, or implementing documentation provisions), *to the extent that*:

____ The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; *and*

____ The group health plan does not create or receive protected health information, except for:

____ Summary health information (§ 164.504(a)); *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.

ii. ____ Subject to the documentation standard and implementation specification only with respect to plan documents amended in accordance with § 164.504(f).