

WHITE PAPER ON HIPAA COMPLIANCE

Prepared by Webster, Chamberlain & Bean
1747 Pennsylvania Ave., N.W.
Washington, D.C. 20006
(202) 785-9500

BACKGROUND

This White Paper is designed to assist in compliance with the privacy requirements imposed by the Health Insurance Portability and Accountability Act (HIPAA). HHS published proposed modifications to the HIPAA Privacy Rule in March 2002, and published the final rule on August 14, 2002, incorporating many of the proposed modifications. Although these final rules take effect on October 15, 2002, the compliance dates for initial implementation of the privacy standards are not affected. Health care providers, health care clearinghouses and health plans (except for small health plans) must comply with the final rules by April 14, 2003. Small health plans, defined as those plans with annual receipts of less than \$5 million, must comply no later than April 14, 2004.

Many state privacy laws continue to apply. This White Paper does *not* include a review of state laws or regulations that may also apply in addition to HIPAA. The exhibits attached to this White Paper do *not* necessarily meet the requirements of your state's laws. Therefore, you are advised to consult with legal counsel or advisors familiar with your state's laws to determine which state laws and regulations will impact you and your practice.

HIPAA IN GENERAL

HIPAA was passed in 1996 to mandate how healthcare plans, providers and clearinghouses store and transmit individuals' personal healthcare information. The two rules fall under one of the general categories of HIPAA known as the Administrative Simplification Act.

The Privacy Rule essentially controls the use and disclosure of what is known as protected health information ("PHI"). PHI, with few exceptions, includes individually identifiable health information held or disclosed by an entity regardless of how it is communicated (e.g., electronically, verbally or written). The Security Rule focuses on requirements for covered entities (including medical practices) to protect and safeguard the confidentiality of medical information. The Security Rule specifically addresses the transmission, storage and receipt of data. Specifically, the Rule regulates a covered entity's computer network, access to it and the method by which it stores and handles data.

The HIPAA rules apply only to “covered entities,” as defined under HIPAA. Under HIPAA, “covered entity” is defined as a health plan, healthcare provider, or a healthcare clearinghouse who transmit any health information in electronic form in connection with a HIPAA transaction. Healthcare includes, but is not limited to, preventive, diagnostic, therapeutic, rehabilitative maintenance, or palliative care, and counseling service, assessment, or procedure with respect to the physical or mental condition, or functional status, or an individual or that affects the structure or function of the body; and sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription. Non-covered entities that request PHI from covered entities will also need to understand HIPAA’s provisions.

HIPAA uses an “opt-in” standard to regulate most uses and disclosures of individually identifiable PHI. Only the information of individuals that is used for personal, family, or household purposes is regulated under HIPAA. Information regarding businesses is not protected under HIPAA.

While one of the major purposes of HIPAA is to provide patients access to their medical records, the Rule also permits healthcare providers to use and disclose PHI about a patient in order to carry out the treatment, payment or healthcare operations (“TPO”) of that provider’s practice. This right to use and disclose PHI is valid as long as the provider makes a good faith effort to obtain written acknowledgement from the patient that he or she has received a copy of the Notice of Privacy Practices. Additionally, healthcare providers may disclose PHI to other healthcare providers for the treatment activities of that provider, and may disclose PHI for the payment activities and certain operational activities (*e.g.*, quality assurance) of that other healthcare provider.

TPO refers to the treatment, payment or healthcare operations of a practice. Treatment is defined as the provision, coordination or management of healthcare and related services by one or more healthcare providers or the referral of a patient for healthcare from one provider to another. Payments is defined as the activities conducted by the practice to obtain reimbursement for healthcare services. This includes billing, claims management, collection activities, verification of insurance coverage, and precertification of services. Healthcare operations is defined as activities related to a provider’s business and clinical management and administrative duties. Some examples include quality assurance, quality improvement, case management training programs, licensing, credentialing, certification, accreditation, compliance programs, business management and general administrative activities of the practice. Generally, uses or disclosures not for TPO purposes requires an authorization from the patient.

Providers requiring assistance from outside entities to accomplish some or all of their business activities and functions will be required to get signed business associate agreements from these entities if they will use or disclose PHI to carry out these functions or activities.

BASIC HIPAA CONCEPTS THAT APPLY TO COVERED ENTITIES AND AFFECT NON-COVERED ENTITIES THAT REQUEST PHI FROM COVERED ENTITIES

Personal Representative

Under HIPAA, a personal representative is treated as if he or she is the individual who is the subject of the PHI. “Decisions related to healthcare,” under the Privacy Rule, refers to making treatment and payment decisions on behalf of the patient. The Privacy Rule provides the following example: a husband may have the authority to make decisions about his wife’s healthcare in an emergency; however, he may not have the right to access PHI related to treatment she received ten years ago.

Minors

The rules make clear that state or other applicable law governs the disclosure of PHI about a minor to their parents. The final rules ensure that HIPAA does not prohibit a covered entity from providing a parent with access to a minor child’s PHI where the parent is technically not the “personal representative” of the child, as long as providing such access is consistent with state or other applicable law.

The “Minimum Necessary” Rule

The Privacy Rule requires covered entities to make reasonable efforts to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose. However, the final rule makes clear that the minimum necessary standard is intended to be both reasonable and flexible. The rule permits a covered entity to rely on the judgment of certain parties requesting the disclosure as to the minimum amount of information that is needed. The rule contains some exceptions – the requirements do not apply to uses or disclosures that are required by law, disclosures made to the individual or pursuant to an authorization initiated by the individual, disclosures to or requests by a health care provider for treatment purposes, uses or disclosures that are required for compliance with the regulations implementing the other administration simplification provisions of HIPAA, or disclosures to the Secretary of HHS for enforcement purposes. The final rules provide that uses and disclosures made pursuant to an authorization are exempt from the minimum necessary standard, regardless of the purpose for which the authorization is obtained. The final rules also contain a new provision which explicitly permits certain incidental uses and disclosures that occur as a result of an otherwise permitted use or disclosure under the Privacy Rule. Finally, the final rules require covered entities to develop criteria that will limit non-routine requests for PHI to information reasonably necessary to accomplish the purpose, and use that criteria to individually review requests.

Disclosures of PHI For Another Covered Entity's TPO

The previous Privacy Rule required a covered entity to obtain an authorization from the individual before it could disclose PHI for purposes of another covered entity's treatment, payment or health care operations ("TPO"). Commentators suggested that this provision impeded the ability of covered entities to obtain reimbursement for health care, to conduct quality assurance or improvement activities, or to monitor fraud and abuse. Commentators also expressed the concern that the rule would have prevented third-party collectors, as business associates of multiple providers, from using a patient's demographic information received from one provider in order to facilitate collection for another provider's payment purposes.

Therefore, the final rules permit covered entities to use or disclose PHI without obtaining an authorization for their own treatment, payment and health care operations functions. Treatment includes the coordination and management of health care among health care providers or by a health care provider with a third party, consultations between health care providers, and referrals of a patient for health care from one health care provider to another. HIPAA's definition of health care operations include conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting certain health care training programs and training non-health care professionals, accreditation, certification, licensing, or credentialing activities; health care fraud and abuse detection and compliance. The final rules also permit a covered entity to disclose PHI for the treatment purposes of any health care provider.

The final rules also state that the following would not require authorizations: (1) a covered entity could disclose PHI for its own TPO; (2) a covered entity may share PHI for the treatment activities of another health care provider; (3) a covered entity may disclose PHI to another covered entity or health care provider for the payment activities of that entity (thus, disclosures of PHI to both covered and non-covered health care providers is permitted); and (4) a covered entity may disclose PHI about an individual to another covered entity for certain health care operations purposes of the covered entity that receives the information, but only to the extent that each entity has, or has had, a relationship with the individual who is the subject of the information being requested, and the request relates to that relationship. The final rules permit such disclosures only for the activities described in paragraphs (1) and (2) of HIPAA's definition of "health care operations," as well as for health care fraud and abuse detection and compliance programs (as provided for in paragraph (4) of HIPAA's definition of "health care

operations.”). This provision is intended to allow information to flow from one covered entity to another for activities important to providing quality and effective health care.

Covered entities are permitted to disclose PHI for treatment purposes regardless of to whom the disclosure is made (i.e., non-covered entity). Covered entities are also permitted to disclose PHI, without an authorization, for payment purposes to other covered entities or any health care provider. However, the rules regarding disclosure of PHI for health care operations are slightly different.

I. Non-covered Entities

Under HIPAA, HHS has jurisdiction only over covered entities. Additionally, HHS has no direct jurisdiction over business associates. A non-covered entity does *not* become a covered entity by providing PHI to a covered entity.

However, a non-covered entity that wants to *obtain* PHI from a health care provider, health plan or health care clearinghouse (covered entities), must obtain the consumer’s authorization.

An authorization is required for use and disclosure of PHI not otherwise allowed by the rule. In general, this means that an authorization is required for purposes that are not part of TPO and not described in § 164.510 or § 164.512. *All* covered entities, not just health care providers, must obtain an authorization to use or disclose PHI for these purposes. For example, a covered entity would need an authorization from individuals to sell a mailing list, to disclose information to an employer for employment decisions, or to disclose information for eligibility for life insurance. A covered entity will never need to obtain both an individual’s consent and authorization for a single use or disclosure. However, a provider may have to obtain consent and authorization from the same patient for different uses or disclosures. HHS has stated that although covered entities need not obtain consents, HHS will strictly enforce the requirement for obtaining an individual’s authorization for uses and disclosures of PHI for purposes not otherwise permitted or required by the Privacy Rule.

An authorization is a more customized document that gives covered entities permission to use specified PHI for specified purposes, which are generally other than TPO, or to disclose PHI to a third party specified by the individual. An authorization is more detailed and specific than a consent and covers only the uses and disclosures and only the PHI stipulated in the authorization. An authorization has an expiration date, and in some cases, it also states the purpose for which the information may be used or disclosed. An authorization may not be revoked if the covered entity acted in reliance on the authorization, or if the authorization was obtained as a condition of obtaining insurance coverage and other law gives the insurer the right to contest the claim or the policy itself.

The necessary elements of an HHS compliant authorization are set forth in section 508 of the Regulations. Briefly, the authorization must provide:

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
2. The name or other specific identification of the person(s) or class of persons, authorized to make the requested use or disclosure;
3. The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;
4. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;
5. A description of each purpose of the requested use or disclosure;
6. A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;
7. A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by this rule;
8. Signature of the individual and date;
9. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual; and
10. If an authorization is requested by a covered entity for its own use or disclosure of PHI that it maintains, the following requirements must be met in addition to those above:
 - a. For any authorization to which the prohibition on conditioning applies, a statement that the covered entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure;
 - b. A description of each purpose of the requested use or disclosure;
 - c. A statement that the individual may inspect or copy the PHI to be used or disclosed, and refuse to sign the authorization;
 - d. If use or disclosure of the PHI will result in direct or indirect

remuneration to the covered entity from a third party, a statement that such remuneration will result.

11. A statement on the covered entity's ability or inability to condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure and a statement regarding the consequences to the individual, if any, of failure to sign the authorization.
12. If a covered entity that creates PHI for the purpose, in whole or in part, of research that includes treatment of individuals, they must obtain an authorization for the use or disclosure of such PHI that contains additional elements, in addition to those listed above. *See* § 164.508(f).

A valid authorization may contain elements or information in addition to the elements listed above, provided that such additional elements or information are not inconsistent with the elements required by the rule. A copy of the signed authorization must be provided to the individual.

If a covered entity seeks an authorization for marketing purposes where the marketing is expected to result in remuneration from a third party, the covered entity is required to disclose the remuneration to the individual.

Suggested authorization language is set forth in Exhibit A.

The final rules simplify the requirements for authorizations by establishing a single set of content requirements that apply to all authorizations regardless of the purpose for which the authorization is sought.

Uses and disclosures of psychotherapy notes are permitted by the final rules without an authorization if they relate to functions of the covered entity and are not for the functions of another covered entity.

Under the final rules, a revocation does not take effect where the authorization was obtained as a condition of obtaining insurance coverage and other law permits the insurer to contest a claim under the policy or the policy itself.

II. Covered Entities

Covered entities include health care providers, health plans and health care clearinghouses. Covered entities have until April 14, 2003 to come into compliance with HIPAA (small health plans have until April 14, 2004).

The HIPAA regulations generally require of covered entities:

1. The issuance of a separate set of privacy disclosures to individuals about whom PHI is collected and/or disclosed and, for health care providers only, a good faith effort to obtain a written acknowledgement that the individual received the health care provider's privacy notice;
2. The receipt of an affirmative "opt-in" authorization from an individual before protected health information may be used or disclosed (subject to a number of exceptions);
3. Compliance with requests by individuals to provide access to their protected health information and to correct or amend this information, if necessary; and
4. Compliance with administrative requirements (*e.g.*, designating a privacy compliance officer, instituting policies and procedures to make sure any PHI that is disclosed is the "minimum necessary" to accomplish the purpose of the disclosure).

Covered entities must also comply with the "minimum necessary" provision of HIPAA. See the discussion above under "HIPAA IN GENERAL" for more information on this provision. Under § 164.502(b), a covered entity must make reasonable efforts to limit disclosure of PHI to "the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." The "minimum necessary" standard also applies to disclosures by covered entities to business associates. The Privacy Rule exempts from the "minimum necessary" requirement uses or disclosures that are authorized by an individual. This includes authorizations covered entities may receive directly from third parties. For example, if a covered entity receives an individual's authorization to disclose PHI to a life insurer for underwriting purposes, the covered entity is permitted to disclose the information requested on the authorization without making any minimum necessary determination. The "minimum necessary" standard also does not apply to disclosures between providers in the context of treatment.

A. Notice of Privacy Practices

Covered entities must provide individuals with a notice of privacy practices. Covered health care providers are required to obtain an individual's written acknowledgement of receipt of such notice of privacy practices. However, in an emergency treatment situation, a covered health care provider with a direct treatment relationship need only make a good faith effort to obtain an individual's "written acknowledgement" of receipt of the provider's privacy notice. If the written

acknowledgement is not obtained, the provider must document its good faith efforts and the reason why the acknowledgement was not obtained. Other covered entities are not required to obtain written acknowledgements, but may choose to obtain an individual's receipt of their privacy notices if they wish. The notice must:

1. Be in plain language;
2. Include a specific header statement;
3. Include description, including at least one example, regarding uses and disclosures of PHI for treatment, payment and health care operations ("TPO"); it must reflect more stringent state or federal law, as applicable, and contain sufficient detail to place individual on notice of the uses/disclosures permitted or required; description of each other purpose for which covered entity may make, use or disclose PHI without consent or authorization;
4. Include statement that other uses or disclosures will be made only with the individual's written authorization, and that authorization may be revoked;
5. Include an explanation of an individual's privacy rights;
6. Include a statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with a notice of its legal duties and privacy practices with respect to PHI;
7. Include a statement that the covered entity is required to abide by the terms of the notice currently in effect;
8. Include a statement that the covered entity reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains;
9. Include a statement describing how it will provide individuals with a revised notice;
10. Include how to file complaints with the covered entity or Secretary of HHS;
11. Include the name or title and phone number of a contact person for more information; and
12. Include the effective date of the notice.

The covered entity must revise its privacy practices notice with any material change to the entity's privacy practices. Any change may not be implemented prior to the effective date of the revised notice.

A covered entity that maintains a Web site providing information about the covered entity's customer services or benefits must prominently post its notice on, and make it available through, the Web site.

Covered health care providers, with one exception, are required to make a good faith effort to obtain a written acknowledgment of the notice at the time of first service delivery – the same time that the notice must be provided. Except in an emergency situation, the health care provider with a direct treatment relationship must make a good faith effort to obtain an individual's "written acknowledgement" or receipt of the privacy notice. If the acknowledgement cannot be obtained, the health care provider must document its good faith effort and note the reason why the acknowledgement could not be obtained. In an emergency situation, the final rules delay the requirement for provision of notice until reasonably practicable after the emergency treatment situation. The notice must be available at the service delivery site for distribution upon request and posted in a prominent location.

The final rules do not prescribe in detail the form the acknowledgment must take. Rather, the rules state only that the acknowledgment be in writing, and intend to allow each covered health care provider to choose the form and other details of the acknowledgment that are best suited to the entity's practices and that will not pose an impediment to the delivery of timely, quality health care. An acknowledgment under the final rules may be obtained, for example, by having the individual sign a separate list or simply initial a cover sheet of the notice to be retained by the covered entity. The final rules do not require the individual's signature on the notice itself. The final rules do not limit the manner in which a covered entity obtains the individual's acknowledgment of receipt of the notice.

Failure by a covered entity to obtain an individual's acknowledgment, assuming it documented its good faith effort, would not be considered a violation of the Privacy Rule and would not interfere with the provider's ability to deliver timely and effective treatment.

Covered entities must maintain copies of the notices issued for six years.

A sample notice of privacy policies is set forth in Exhibit B.

B. Consents

Under the final rules, covered entities with a direct treatment relationship with the individual are not required to obtain a consent prior to using and disclosing PHI for TPO. However, as discussed above, health care providers are required to make a good faith

effort to obtain a written acknowledgement that the individual has received a notice of privacy practices.

Health plans and clearinghouses may also use and disclose PHI for purposes of TPO¹ without obtaining consent. However, these entities are permitted to obtain consent.

In all other contexts, covered entities must obtain authorizations (e.g., marketing). Authorizations must be written in specific terms and may even allow use and disclosure of PHI by third parties.

A consent is a general document that gives covered entities permission to use and disclose all PHI for TPO. It gives permission only to that provider, not to any other person. Health care providers may condition the provision of treatment on the individual providing consent. One consent may cover all uses and disclosures for TPO by that provider, indefinitely. A consent need not specify the particular information to be used or disclosed, nor the recipients of disclosed information. The prior privacy rule's requirements relating to the format and content of consents have been eliminated. The final rules give covered entities that choose to obtain consents complete discretion to design consents.

Sample consent language, which conforms to the previous privacy rule, is set forth in Exhibit C. However, because the final rules give covered entities complete discretion to design consents that best suit their needs, all of the provisions in the consent in Exhibit C need *not* be used. It bears repeating that a consent pertains to disclosures *only* for the purpose of "treatment," "payment" and "health care operations." A consent allows use and disclosure of protected health information by the covered entity seeking the consent, not by other persons. A covered entity cannot use or disclose protected health information beyond what is covered in the consent. Covered entities (other than health care providers), may, at their option, obtain consent; if no consent is obtained, the covered entity may use or disclose protected health information only to carry out treatment, payment, and health care operations as otherwise permitted under the rule and consistent with its notice of privacy practices.

An individual may request restrictions on the uses or disclosures of health information for TPO. However, the covered entity need not agree to the restriction requested, but is bound by any restriction to which it agrees.

A covered entity must retain the signed consent for six years from the date it was last in effect. Transition provisions allow providers to rely on consents received prior to April 14, 2003 for uses and disclosures of PHI obtained prior to that date.

¹ Common "payment" activities include, but are not limited to, determining eligibility or coverage under a plan and adjudicating claims; risk adjustments; billing and collection activities, reviewing health care services for medical necessity, coverage, justification of charges, and the like; disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about the covered entity).

C. Authorizations

See the discussion regarding authorizations above under Non-Covered Entities.

A sample authorization is set forth in Exhibit A.

III. Hybrid Entities

A hybrid entity is a single legal entity whose business activities include both covered and non-covered functions, regardless of what proportion of the entity's functions are covered.

The final rules permit a covered entity with both covered and non-covered functions to elect whether to be treated as a hybrid entity. If the entity chooses to be a hybrid entity, it is required to designate health care components and establish firewalls to guard against use or disclosure of PHI within the entity. The requirements of HIPAA would then apply only to the health care components of the entity. However, if the entity is a hybrid entity, intracorporate disclosures of PHI are prohibited (unless those uses or disclosures could otherwise be made without an authorization) absent a valid authorization. If the covered entity chooses not to be a hybrid entity, HIPAA's requirements apply to the entire entity.

If a covered entity elects to be treated as a hybrid entity, authorization is not required for uses and disclosures made *to* non-health related divisions of the covered entity if the uses or disclosures could otherwise be made without authorization. If a covered entity elects to be treated as a hybrid company, it will need to obtain a HIPAA compliant authorization to *obtain* PHI, including any PHI held by another division of the company that is subject to the HHS Regulations.

The final rules modified the definition of "health care component" to make it clear that a hybrid entity may determine for itself which components of the entity it will designate as one or more health care components. However, the entity must designate as a health care component any component that would meet the definition of "covered entity" if it were a separate legal entity. A hybrid entity may, but is not required to, treat its "business associate" functions as health care components. It is assumed that covered entities will include its business associate functions in its health care components because a covered entity cannot have business associate agreements with itself and, therefore, disclosures could only be made pursuant to an authorization.

The definition of "PHI" has been amended to clarify that PHI does not include employment records held by a covered entity in its role as employer. This amendment eliminates the need for a covered entity to designate itself as a hybrid entity to ensure that its employment records are not treated as PHI.

The necessary elements of an HHS compliant authorization are set forth in section 508 of the Regulations, and are discussed above under the Non-Covered Entity Section.

Suggested authorization language is set forth in Exhibit A.

IV. Business Associates (45 CFR §§ 160.103, 164.502(e), 164.514(e))

An individual or company (whether a covered entity or non-covered entity) becomes a business associate of a covered entity if its functions and activities are those that involve the use or disclosure of individually identifiable health information and include claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing. The regulations state that a business associate also is one who provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

Specifically, a business associate is:

1. A person or entity who provides certain functions, activities, or services for or to a covered entity, involving the use and/or disclosure of PHI.
2. Not a member of the health care provider, health plan or other covered entity's workforce.
3. A health care provider, health plan, or other covered entity can also be a business associate to another covered entity.
4. Exceptions – the business associate requirements do not apply to covered entities who disclose PHI to providers for treatment purposes (*e.g.*, information exchanges between a hospital and physicians with admitting privileges at the hospital).

In allowing covered entities to give PHI to business associates, the rule conditions such disclosures on the covered entity obtaining, typically by contract, satisfactory assurances that the business associate will use the information only for the purposes for which they were engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with the covered entity's duties to provide individuals with access to PHI about them and a history of disclosures. PHI may be disclosed to a business associate *only* to help the covered entity carry out its health care functions – not for independent use by the business associate.

A business associate contract must:

1. Establish the permitted and required uses and disclosures of PHI by the business associate. The contract may not authorize the business associate to use or further disclose the PHI in a manner that would violate the requirements of § 164.504(e)(1) except that:
 - a. The contract may permit the business associate to use and disclose PHI for the proper management and administration of the business associate; and
 - b. The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.
2. Provide that the business associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law;
3. Provide that the business associate will use appropriate safeguards to prevent use or disclosure of the PHI other than as provided by in the contract;
4. Provide that the business associate report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;
5. Ensure that any agents or subcontractors to whom the business associate provides PHI received from, or created or received by the business associate on behalf of the covered entity agrees to the same restrictions and conditions that apply to the business associate;
6. Make available PHI in accordance with § 164.524;
7. Make available PHI for amendment and incorporate any amendments to PHI in accordance with § 164.526;
8. Make available the PHI required to provide an accounting of disclosures in accordance with § 164.528;
9. Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary of HHS for the purposes of determining the covered entity's compliance;
10. Provide that at termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the business associate on behalf of the covered entity, that the business associate still maintains in

any form and retain no copies of such information, or if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible;

11. Authorize termination of the contract by the covered entity if the covered entity determines that the business associate has violated a material term of the contract.

A sample business associate contract is set forth in Exhibit D.

The final rules at § 164.532(d) and (e) allow covered entities (other than small health plans) to continue to operate under certain existing contracts with business associates for up to one year beyond the April 14, 2003 compliance date of the Privacy Rule.

The additional transition period would be available to a covered entity, other than a small health plan, if, prior to the effective date of this transition provision, the covered entity has an existing contract or other written arrangement with a business associate, and such contract or agreement is not renewed or modified between the effective date of this provision and the Privacy Rule's compliance date of April 14, 2003. The final rules deem such contracts to be compliant with the Privacy Rule until either the covered entity has renewed or modified the contract following the compliance date of the Privacy Rule (April 14, 2003), or April 14, 2004, whichever is sooner. In cases where a contract simply renews automatically without any change in terms or other action by the parties (an "evergreen contract"), HHS intends that such contracts would be eligible for the extension and that deemed compliance would not terminate when these contracts automatically roll over. All business associate agreements must be compliant by 2004. Please note that the extension for amending agreements does *not* relieve covered entities of ensuring that their business associate complies with HIPAA's requirements by the April 14, 2003 compliance date. Covered entities are also not relieved of their obligations to mitigate, whenever possible, any harmful effect resulting from a business associate's use or disclosure of PHI in contravention of policies, procedures or HIPAA. Beginning April 14, 2003, covered entities are required to ensure the necessary cooperation of the business associates, but are not required to obtain written satisfactory assurances. The agreements are deemed to fulfill the satisfactory assurance requirement during the transition period.

The final rules contain model business associate contract provisions. Covered entities are not required to use any of the model provisions; they were provided by HHS to help compliance by covered entities. These provisions are attached as Exhibit E.