



EMPLOYEE BENEFIT SERVICE CENTER

3150 Carlisle Blvd. NE, Suite 203 Albuquerque, NM 87110
Phone (505) 889-4506 Fax (505) 889-4599
E-mail: helpdesk@ebsc.net

**HIPAA Privacy Manual
for
Employee Benefit Service Center**

TABLE OF CONTENTS

| | Page |
|--|-----------|
| Overview of HIPAA's Administrative Simplification Provisions..... | 1 |
| 1. Electronic Data Interchange (" <i>EDI</i> ") Transaction Standards..... | 1 |
| 2. Identifier Standards..... | 1 |
| 3. Security and Electronic Signature Standards..... | 1 |
| 4. Privacy of Protected Health Information..... | 1 |
| HIPAA's Privacy Standards in General..... | 2 |
| 1. What is Protected Health Information?..... | 2 |
| 2. What is a Limited Data Set?..... | 2 |
| 3. When is health information <u>not</u> Protected Health Information?..... | 4 |
| 4. Who are Covered Entities?..... | 5 |
| 5. Is an Employer a Covered Entity?..... | 5 |
| 6. How do the Privacy Standards apply to Third Party Administrators? Who are Business Associates?..... | 5 |
| Use and Disclosure of Protected Health Information in General..... | 7 |
| 1. What are required disclosures?..... | 7 |
| 2. What are permitted uses and disclosures?..... | 7 |
| 3. When is consent required?..... | 8 |
| 4. What is TPO?..... | 9 |
| 5. When is an authorization required or recommended?..... | 10 |
| Use and Disclosure of Protected Health Information in Specific Situations..... | 13 |
| 1. How do the Privacy Standards apply to uses and disclosures by employers?..... | 13 |
| A. The Employer as the Plan Sponsor..... | 13 |
| B. The Employer as the Plan Administrator..... | 14 |
| 2. How do the Privacy Standards apply to disclosures to plan participants?..... | 15 |
| 3. How do the Privacy Standards apply to disclosures to family members of participants?..... | 15 |
| 4. How do the Privacy Standards apply to disclosures to representatives of participants?..... | 16 |
| 5. How do the Privacy Standards apply to disclosures to medical providers?..... | 17 |
| 6. How do the Privacy Standards apply to disclosures to MGUs and stop-loss carriers?..... | 17 |
| 7. How do the Privacy Standards apply to disclosures to other third-party vendors, such as PPOs, utilization review companies, prescription drug vendors, etc.?..... | 18 |
| 8. How do the Privacy Standards apply to disclosures to a TPA's advisors, such as attorneys?..... | 19 |
| 9. Does the plan have a duty to verify the identity of an individual or entity requesting PHI before disclosure?..... | 20 |
| Health Plan Compliance with the Privacy Standards..... | 22 |
| 1. Enter into Business Associate Agreements with each Business Associate..... | 22 |
| 2. Obtain any authorizations that may be needed..... | 23 |
| 3. Amend the Plan Document and Summary Plan Description..... | 23 |
| 4. Adopt procedures to comply with the "minimum necessary" requirements..... | 24 |
| 5. Establish firewalls; limit employees with access to PHI..... | 25 |
| 6. Designate a privacy official..... | 26 |
| 7. Designate a contact person for complaints and notices..... | 27 |

| | |
|---|----|
| 8. Institute procedures for resolving, and sanctions for, improper use or disclosure..... | 27 |
| 9. Comply with participants' rights regarding PHI..... | 27 |
| 10. Respond to requests by HHS. | 28 |
| 11. Institute procedures for destruction or maintenance of PHI. | 28 |
| 12. Certify compliance..... | 28 |
| 13. Distribute the Notice of Privacy Practices. | 28 |

Other Operational Issues 29

| | |
|---|----|
| 1. Do the HIPAA regulations conflict with the U.S. Department of Labor's new Claims Regulations? If so, how do we handle those conflicts? | 29 |
| 2. What are the "reasonable safeguards" we must take?..... | 30 |
| 3. What are the penalties for non-compliance?..... | 30 |

NOTE: We advise consulting with your TPA before utilizing any of the Exhibits contained in this Manual. Your TPA may work to revise any exhibits to customize them to your plan's needs.

Exhibits:

| | |
|------------|---|
| Exhibit A: | Form of Authorization |
| Exhibit B: | Form of Plan Amendment |
| Exhibit C: | Form of Plan Sponsor Certification |
| Exhibit D: | Suggested Procedures for Separation of Plan and Plan Sponsor |
| Exhibit E: | Form for Designation of Authorized Representative |
| Exhibit F: | Form of Business Associate Agreement |
| Exhibit G: | Suggested Verification Procedures |
| Exhibit H: | Minimum Necessary Requirements – Recommended Guidelines for Plan Administrators |
| Exhibit I: | Firewalls and Employee Access – Checklist of Items for the Employer to Consider |
| Exhibit J: | Form for Tracking PHI Uses, Disclosures and Requests |
| Exhibit K: | Guidelines and Forms Related to Participants' Rights Regarding PHI |
| Exhibit L: | Suggested Guidelines Regarding Violations |
| Exhibit M: | Form of Notice of Privacy Practices |
| Exhibit N: | Suggested Procedures for Destruction or Maintenance of PHI |

Overview of HIPAA's Administrative Simplification Provisions

The Health Insurance Portability and Accountability Act of 1996, as amended ("*HIPAA*") contains four "administrative simplification" provisions, which will take effect over the next several years, as follows:

1. Electronic Data Interchange ("*EDI*") Transaction Standards. Electronic Data Interchange ("*EDI*") Transaction Standards, which address the electronic transmission of health care data, will take effect on October 16, 2002*, unless a compliance plan is filed with the U.S. Department of Health and Human Services ("*HHS*") by that date, in which case the effective date is October 16, 2003. Earlier this year, HHS published a model form to be used for the compliance plan; however, on May 31, 2002, HHS announced that it is redesigning the form. Nonetheless, HHS recently indicated that they have decided not to redesign the form. In addition, on that same date, HHS issued a proposed rule with changes to the transaction standards. No date has been given for when the final rule will be available.

The EDI Transaction Standards also include **Medical Data Code Set Standards**, relating to the code sets for data elements such as claims, diseases, conditions, payment and referral information, which are widely used in the health care industry. On May 31, 2002, HHS proposed rules that would repeal the NDC code as the standard code set to refer to drugs.

2. Identifier Standards. Identifier Standards (for employers, health plans, individuals and health care providers).

- On May 31, 2002, a final rule was issued establishing the federal employer identification number (EIN) as the standard unique identifier for employers. Covered Entities must comply with this rule no later than July 30, 2004.*
- Proposed rules were issued in May 1998 to establish identifier standards for health care providers; recommendations for an identifier for individuals were published by HHS in July 1997. The provisions in the proposed rules will take effect 60 days after final rules are published, and health plans will then have two years* before they must comply.
- No regulations have been proposed regarding health plan identifiers.

3. Security and Electronic Signature Standards. Proposed rules were issued in 1998 to establish standards for the security of health information and electronic signatures. They will become effective two years* after final rules are published.

4. Privacy of Protected Health Information. HHS issued a Final Rule implementing HIPAA's Standards for Privacy of Individually Identifiable Health Information (*the "Privacy Standards"*) on December 28, 2000; the Privacy Standards will take effect on April 14, 2003.* On July 6, 2001, it published "guidance" to address frequently asked questions as well as problems that it had identified in the Final Rule. On March 27, 2002, HHS issued a Proposed Rule that would modify certain of the Privacy Standards (including giving Covered Entities an additional year, until April 14, 2004, to amend their existing contracts with Business Associates.) Comments were accepted regarding the Proposed Rule until April 26, 2002. The Proposed Rule was issued in final form on August 14, 2002 (the "Amendments"). HHS has announced that it will issue additional guidance regarding the Privacy Standards, including the Amendments, in the next several months.

*There is a one-year delay from these dates for "small health plans," which are plans with annual receipts of less than \$6 million. HHS has yet to define what "annual receipts" are in the context of a health plan, and refers only to regulations issued by the Small Business Administration ("SBA"). Discussions with the SBA indicate that, if a health plan is established on a not-for-profit basis, then it does not fall within the definition of a "small health plan." On the other hand, if it is a for-profit entity, then the \$6 million is measured by taking into account the total income of the Plan Sponsor, together with all of its affiliates (based upon an average of its three most recently completed fiscal years). We have been advised that HHS is planning on issuing guidance on this issue, and we will continue to watch for it.

HIPAA's Privacy Standards in General

The Privacy Standards are designed to protect each individual's individually identifiable health information ("*Protected Health Information*" or "*PHI*") from being used or disclosed by Covered Entities without the individual's express authorization, except as explicitly permitted or required in certain limited circumstances. If health information does not meet the definition of Protected Health Information, then the Privacy Standards do not apply to that information.

Generally, the Privacy Standards restrict how a Covered Entity (essentially, health plans, health care providers who transmit health information in electronic form and health care clearinghouses) may use and disclose PHI – including when a use or disclosure is required or permitted – and the conditions relating to the use or disclosure. Covered Entities' use or disclosure of, or requests for, PHI must consist of only the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request.

The Privacy Standards also apply to Business Associates (a person who, on behalf of a Covered Entity, performs or helps with an activity involving the use or disclosure of individually identifiable health information) of Covered Entities, by virtue of a Business Associate Agreement, which is required by the Privacy Standards to be in place between those two parties.

1. What is Protected Health Information?

"*Protected Health Information*" is health information that is created or received by a Covered Entity, or employer, and relates to:

- A person's past, present or future physical or mental health;
- Provision of health care to that person; or
- Past, present or future payment for that person's health care.

Furthermore, to be "*Protected Health Information*," the information also must be "individually identifiable health information," which means that, in addition to the above requirements, the health information must identify the individual or a reasonable basis must exist to believe that an individual can be identified using the information. "*Protected Health Information*" covers information in any form – electronic, oral or written.

2. What is a Limited Data Set?

A "*Limited Data Set*" is Protected Health Information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

- Names;
- Postal address information, other than town or city, state, and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;

- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

A Covered Entity may use or disclose a Limited Data Set only for the purposes of research, public health, or health care operations. Additionally, a Covered Entity may use PHI to create a Limited Data Set, or disclose PHI only to a Business Associate for such purpose, whether or not the Limited Data Set is to be used by the Covered Entity. However, before a Covered Entity may use or disclose a Limited Data Set, the Covered Entity must enter into a "*Data Use Agreement*" with the recipient of the Limited Data Set. The Data Use Agreement must:

- Establish the permitted uses and disclosures of such information by the recipient of the Limited Data Set as set forth above—the agreement may not authorize the recipient of the Limited Data Set to use or further disclose the information in a manner that would violate the requirements of the Privacy Standards, if done by the Covered Entity;
- Establish who is permitted to use or receive the Limited Data Set; and
- Provide that the recipient of the Limited Data Set will:
 - Not use or further disclose the information other than as permitted by the Data Use Agreement or as otherwise required by law;
 - Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the Data Use Agreement;
 - Report to the Covered Entity any use or disclosure of the information not provided for by its Data Use Agreement of which it becomes aware;
 - Ensure that any agents, including a subcontractor, to whom it provides the Limited Data Set agrees to the same restrictions and conditions that apply to the recipient of the Limited Data Set with respect to such information; and
 - Not identify the information or contact the individuals.

A Covered Entity is not in compliance with the Privacy Standards if the Covered Entity knew of a pattern of activity or practice of the recipient of the Limited Data Set that constituted a material breach or violation of the Data Use Agreement, unless the Covered Entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

- Discontinued disclosure of PHI to the recipient of the Limited Data Set; and
- Reported the problem to the Secretary of HHS.

A Covered Entity that is a recipient of a Limited Data Set and violates a Data Use Agreement will be in non-compliance with the Privacy Standards. We are not providing a form of Data Use Agreement because it appears from the preamble to the Amendments that the rules regarding Limited Data Sets and Data Use Agreements are intended to apply in research and analyses situations, which we believe will be inapplicable for health plans.

3. *When is health information not Protected Health Information?*

Health information is not PHI, and is considered to be "de-identified" if it is not "individually identifiable health information." If information has been de-identified, then the information is not subject to the Privacy Standards.

Someone who is not familiar with the Privacy Standards may look at health information and mistakenly think that it is de-identified. For example, a claims history, with all participants' names and Social Security numbers deleted, is not de-identified in accordance with the Privacy Standards. The Privacy Standards contain a strict de-identification requirement, such that all of the following identifiers (whether they relate to the individual or to the individual's employer, relatives or household members) must be deleted for the information to be de-identified:

- Names;
- Geographic subdivisions smaller than a state, including street address, city, county, precinct, and zip code (although the first three digits of some zip codes may be used);
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date and date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Fax numbers;
- Email addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate or license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic or code (unless permitted by the Privacy Standards).

In addition to removing the above identifiers, for information to be properly de-identified, the Privacy Standards require that a Covered Entity must not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

If a health plan cannot meet the above de-identification requirements, the Privacy Standards provide a second method for determining when information is de-identified. This method involves obtaining an expert to determine whether or not the information can be used to identify an individual. The expert must have appropriate knowledge of, and experience with, generally accepted statistical and scientific principles for rendering information not individually identifiable and must determine, based upon that

knowledge and experience, that the risk is very small that the information could be used, either alone or together with other reasonably available information, to identify an individual.

4. *Who are Covered Entities?*

"Covered Entities" are:

- Health care providers who conduct electronic transactions;
- Health plans (both insured and self-insured); and
- Health care clearinghouses.

5. *Is an Employer a Covered Entity?*

At first glance, it appears that an employer is not a Covered Entity. However, by virtue of the employer's typical assumption of the role of Plan Administrator, an employer will come under the definition of a Covered Entity with respect to an employer-sponsored health plan.

It is important to keep in mind the employer's dual functions as Plan Administrator and as Plan Sponsor. When the employer is acting as the Plan Sponsor, it is responsible for establishing, amending, terminating and funding the plan. Because the Plan Sponsor is not a fiduciary, it is not required to make such decisions with the best interests of the plan participants in mind; rather, it may make such decisions as business decisions. On the other hand, when the employer is acting as the Plan Administrator, it is a fiduciary and has the liability associated with that position. As Plan Administrator, it is responsible for all operations of the plan and will have access to PHI. As the Plan Sponsor, it may require that access, but certain safeguards must be in place before access can be permitted in accordance with the Privacy Standards. If you read the Privacy Standards, you will see that HHS neglected to make this differentiation and refers only to the "plan" and the "plan sponsor." When questioned about this omission, HHS representatives have said that the above differentiation is correct, and should be applied in the context of the Privacy Standards.

6. *How do the Privacy Standards apply to Third Party Administrators? Who are Business Associates?*

While TPAs are not Covered Entities, they must comply with certain requirements of the Privacy Standards because they come under the definition of a Business Associate.

A *"Business Associate"* is a person who, on behalf of a Covered Entity, performs or assists with an activity involving the use or disclosure of individually identifiable health information. A *"Business Associate"* includes an individual or entity performing the following functions:

- Claims processing or administration;
- Data analysis, processing or administration;
- Utilization review;
- Quality assurance;
- Billing;
- Benefit management;

- Practice management; and
- Re-pricing.

A "*Business Associate*" also includes service providers who handle PHI, such as those providing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation and financial services to or for the Covered Entity.

A "*Business Associate*" does not include a member of a Covered Entity's workforce.

Use and Disclosure of Protected Health Information in General

The Privacy Standards generally preempt state law provisions that conflict with the Privacy Standards. State laws that do not conflict with the Privacy Standards will apply, and state laws that apply to entities not covered by the Privacy Standards (*e.g.* employers) still may apply. However, the Privacy Standards contain four exceptions to the general rule that they will preempt conflicting state laws. These exceptions are:

- If state law is more stringent than the Privacy Standards;
- If state law provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention;
- If state law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals; or
- If the Secretary of HHS determines that the provisions of the state law are excepted from the general preemption rule.

1. What are required disclosures?

Covered Entities must disclose PHI in two instances:

- PHI must be disclosed to individuals who request access to their own PHI or request an accounting of PHI disclosures.
- PHI must be disclosed when required by HHS to determine if the Covered Entity is in compliance with the Privacy Standards.

2. What are permitted uses and disclosures?

Covered Entities are permitted to use and disclose PHI in the following instances:

- The PHI is used by, or disclosed to, the individual who is the subject of the PHI.
- The use or disclosure is for treatment, payment or health care operations ("*TPO*").
- The use or disclosure is incident to a use or disclosure otherwise permitted or required by the Privacy Standards, provided that the Covered Entity complies with certain "minimum necessary" standards and adopts certain safeguards.
- The use or disclosure is based on, and is in compliance with, a valid authorization.

- The use or disclosure is based on an agreement or otherwise permitted by the Privacy Standards.
- The use or disclosure is explicitly permitted by the Privacy Standards.

3. *When is consent required?*

Although a Covered Entity **may** obtain a consent to use or disclose PHI for purposes of TPO, following the recent Amendments, the Privacy Standards **never require** that a Covered Entity obtain a consent. The original version of the Privacy Standards expressly reflected that a consent can only be used by the Covered Entity who obtains the consent; that is, a consent is not effective to permit another Covered Entity to use or disclose PHI. However, the recent Amendments omit this limit on who may use a consent; nonetheless, taking a conservative approach, we do not recommend that a Covered Entity use or disclose PHI based upon a consent obtained by another Covered Entity unless and until HHS issues guidance clarifying that this may be done.

Moreover, the original version of the Privacy Standards made clear that although consent is not required, if a plan requests that an individual sign a consent that is not sought in conjunction with enrollment and the individual refuses to do so, the plan cannot use or disclose PHI for the purposes indicated in the consent. After the recent Amendments, this is no longer clear; yet we continue to believe that if a plan requests a consent in circumstances unrelated to enrollment and an individual refuses to give consent, the plan is best advised not to use or disclose PHI for the purposes indicated in the requested consent. Additionally, the Privacy Standards originally reflected that if, in conjunction with the enrollment process, a plan asks an individual to sign a consent for TPO purposes and the individual refuses, then the plan may refuse to enroll the individual. However the recent Amendments deleted this provision. Thus, again taking a conservative approach, we do not recommend that plans refuse to enroll persons for declining to sign a requested consent in conjunction with enrollment. Nevertheless, plans can condition enrollment on the signing of an authorization under certain circumstances. See Item 5 below discussing authorizations. Plans may wish to request a consent if they are required to do so under applicable state laws. **Otherwise, we do not recommend that plans request consents from plan participants.**

Although most people use the words "consent" and "authorization" interchangeably, it is important to recognize that under the Privacy Standards, there is a distinction between them, which is explained in more detail in Item 5 below.

Following the recent Amendments, the Privacy Standards allow Covered Entities that choose to have a consent process complete discretion in designing this process, allowing complete flexibility to each Covered Entity. Still, Covered Entities that choose to obtain consent are well advised to adopt as many of the original requirements for consent as possible.¹

¹The Privacy Standards originally reflected that for a consent to be valid, the following requirements must be met:

- The consent form may not be combined with a privacy notice. It may be combined with other documents that request an individual's written legal permission, but if so, then it must be (a) visually separate from the other written legal permission; and (b) separately signed and dated. A consent also may be combined with a research authorization that complies with the Privacy Standards.
- It must be retained, in either written or electronic form, for six years from the later of the date it was created or the date it was last in effect.
- It must permit the individual to revoke it at any time. Any revocation must be in writing and may not be retroactive if the Covered Entity has acted in reliance on the consent.
- It must be in plain language and contain the following specific provisions:
 - Inform the individual that PHI may be used or disclosed for TPO purposes, which must be listed on the form;

We are not providing a form of consent because we do not recommend that it be used unless your state law requires it. In that event, you will need a form of consent that complies with applicable state law.

4. *What is TPO?*²

"TPO" refers to treatment, payment and health care operations.

"Treatment" means the provision, coordination or management of health care and related services by one or more health care providers, including:

- The coordination or management of health care by a health care provider with a third party;
- Consultation between health care providers relating to a patient; or
- The referral of a patient from one health care provider to another.

"Treatment" does not relate to activities of health plans.

"Payment" means activities undertaken by (a) the plan to obtain premiums or determine or fulfill its responsibility for coverage and the provision of plan benefits or (b) a health care provider or plan to obtain or provide reimbursement for the provision of health care. Additionally, the activities must relate to the individual to whom health care is provided. The Privacy Standards set forth various activities that could be considered "payment":

- Eligibility determinations;
- Coverage determinations;
- Coordination of benefits;
- Determination of cost-sharing amounts (such as plan maximums and co-payments);
- Adjudication of health benefit claims, appeals and benefit disputes;
- Subrogation and reimbursement of health benefit claims;
- Risk-adjusting amounts due based on enrollee health status and demographic characteristics;
- Billing, and collection activities;
- Claims management and related health care data processing, including auditing payments, investigating and resolving payment disputes and responding to participant inquiries regarding payments;
- Obtaining payment under a contract for reinsurance, stop-loss insurance or excess loss insurance;

-
- Refer to the privacy notice for a more complete description of permitted uses and disclosures;
 - State that the individual has the right to review the privacy notice before signing the consent;
 - State that the terms of the privacy notice may change and describe how a revised notice may be obtained;
 - State that the individual may request that the Covered Entity restrict how PHI is used or disclosed for TPO purposes, and further advise that the Covered Entity is not required to agree to such restrictions and that if the Covered Entity agrees to the restrictions, it is bound by them;
 - State that the individual may revoke the consent in writing, except to the extent of any reliance by the Covered Entity; and
 - Be signed and dated.

² In speaking with a number of TPA clients regarding TPO, no client was able to identify any service that they provide on behalf of health plans that would not fit within either the definitions of payment or health care operations included under TPO. This is important because, as reflected above, a plan may disclose PHI for TPO purposes without consent or authorization.

- Medical necessity reviews, or reviews of coverage under a health plan, appropriateness of care or justification of charges;
- Utilization review, including precertification, preauthorization, concurrent review and retrospective review; and
- Disclosure of the following information to consumer reporting agencies related to the collection of premiums or reimbursement:
 - Name and address,
 - Date of birth,
 - Social Security number,
 - Payment history,
 - Account number, and
 - Name and address of the provider and/or health plan.

"Payment" would encompass preparation of explanation of benefits (EOB) statements.

"Health care operations" means any of the following activities of a Covered Entity that maintains PHI:

- Quality assessment and improvement activities (including outcomes evaluation and development of clinical guidelines, except if the purpose of studies resulting from such activities is to gain generalized knowledge);
- Population-based activities (which are activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, and contacting 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 and plan performance;
- Underwriting and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, as well as ceding, securing or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess loss insurance);
- Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detections and compliance programs;
- Business planning and development;
- Business management and general administration³; and
- Disease management.

5. When is an authorization required or recommended?

An authorization may allow the use and disclosure of PHI for purposes other than those of TPO. It also may allow such use and disclosure by both the Covered Entity who requests it and by a third party.

³ Business management and general administrative activities include, but are not limited to: (1) management activities relating to implementation of and compliance with the requirements of the Privacy Standards; (2) customer service, including the provision of data analyses for policy holders, Plan Sponsors or other customers, provided that PHI is not disclosed to such policy holder, Plan Sponsor or customer; (3) resolution of internal grievances; (4) the sale, transfer, merger or consolidation of all or part of the Covered Entity with another Covered Entity, or an entity that following such activity will become a Covered Entity, and due diligence related to such activity; and (5) consistent with the applicable requirements of the Privacy Standards, creating de-identified health information or a Limited Data Set, and fundraising for the benefit of the Covered Entity.

Differences between consent and authorization. It is important to recognize the differences between a consent and an authorization. While a consent allows PHI to be used or disclosed only for TPO purposes, an authorization may allow the use and disclosure of PHI for purposes other than TPO. Plans are not required (although they are permitted) to obtain a consent to use or disclose PHI for TPO purposes. However, plans must obtain an authorization to use or disclose PHI for purposes other than TPO. Additionally, consents are written in broad, general terms, but an authorization must contain very specific terms to be valid. Further, as indicated previously, following the recent Amendments, it is unclear whether a consent may only be used by the Covered Entity that obtained it. On the other hand, any party specified in an authorization may use or disclose PHI as long as that use or disclosure is consistent with the terms of the authorization.

Under the Privacy Standards, a health plan may condition enrollment or eligibility for benefits upon provision of an authorization requested by the plan prior to an individual's enrollment in the plan **IF**:

- the authorization is for the plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk-rating determinations, and
- the authorization is not for a use or disclosure of psychotherapy notes.

A health plan is not required to have an authorization to use or disclose PHI for TPO purposes or if the use or disclosure is otherwise required or permitted under the Privacy Standards (as set forth above in Items 1 and 2, respectively, of this section). However, a health plan may want to obtain an authorization if it believes that any of its uses or disclosures of PHI do not fall within the definition of "TPO." If a plan obtains an authorization, the plan may only use and disclose PHI in a manner that is consistent with the authorization. Please note that, except in certain limited circumstances, an authorization is required for any use or disclosure of psychotherapy notes.

For an authorization to be valid, it must be written in plain language and include the following:

- A specific and meaningful description of the information to be used or disclosed;
- The name or other specific identification of the person(s) or class of persons authorized to make the requested use or disclosure;
- 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;
- A description of each purpose of the requested use or disclosure—the statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose;
- Any expiration date or expiration event that relates to the individual or the purpose of the use or disclosure—the statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of PHI for research, including for the creation and maintenance of a research database or research repository;
- If the authorization is for use or disclosure of PHI for marketing in which the Covered Entity will receive a direct or indirect remuneration from a third party, a statement that such remuneration is involved;
- Signature of the individual and the date;
- If the authorization is signed by the individual's personal representative, a description of that representative's authority to act on the individual's behalf must be provided; and
- Statements adequate to place the individual on notice of all of the following:
 - The individual's right to revoke the authorization in writing, and either (a) the exceptions to the right to revoke and a description of how the individual may revoke the authorization; or (b) if those exceptions and the description regarding how to

revoke are included in the Covered Entity's privacy notice, a reference to the privacy notice;

- The ability or inability to condition treatment, payment, or enrollment or eligibility for benefits on the authorization, by stating either (a) the Covered Entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when prohibited by the Privacy Standards, or (b) the consequences to the individual of a refusal to sign the authorization when the Covered Entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization; and
- The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by the Privacy Standards.

The authorization must be retained, either in written or electronic form, for six years from the later of the date it was created or the date it was last in effect. Also, plans must give the individual a copy of the signed authorization.

See Item 1A in the section entitled "Use and Disclosure of Protected Health Information in Specific Situations" for a discussion of if, and when, a plan should request authorizations.

A form of authorization is attached as **Exhibit A**.

Use and Disclosure of Protected Health Information in Specific Situations

1. How do the Privacy Standards apply to uses and disclosures by employers?

As set forth above, the employer typically acts as both the Plan Sponsor and the Plan Administrator. In those two roles, it has different responsibilities and liability and is permitted to use and disclose Protected Health Information differently under the Privacy Standards.

A. The Employer as the Plan Sponsor

When the employer is acting as the Plan Sponsor, it is not a fiduciary and does not have the liability associated with fiduciary status. As the Plan Sponsor, the employer is responsible for establishing, amending, terminating and funding the plan.

As the Plan Sponsor, the employer is not a Covered Entity, and it may use PHI for plan administration purposes only if it completes designated amendments to plan documents and establishes certain procedures. The employer must agree to use and disclose PHI only for the plan administration functions that are specified in the plan documents.⁴ The Privacy Standards require certain plan amendments designed to ensure adequate separation between the plan and the Plan Sponsor and a certification from the Plan Sponsor before the plan may disclose PHI to the Plan Sponsor. A form of plan amendment is attached as **Exhibit B**, and a form of certification is attached as **Exhibit C**.

However, the Plan Sponsor will need PHI for its duties as Plan Sponsor (such as obtaining excess loss insurance), which do not come under the HHS definition of "plan administration functions." Without authorizations, plans may not disclose PHI to the Plan Sponsor for purposes of employment-related functions, such as certification under the Family and Medical Leave Act or fitness to return to work, or functions in connection with any other benefits or benefit plans -- assuming the Plan Sponsor has more than one benefit plan. Item 5 in the section entitled "Use and Disclosure of Protected Health Information In General" sets forth the circumstances under which a plan may condition enrollment and eligibility for benefits upon receipt of an authorization. Further, nothing in the Privacy Standards prohibits an employer from conditioning employment on receipt of appropriate authorizations. Options for when, and if, to obtain authorizations are outlined below.

It is important that the employer understand that information it receives in its role as Plan Administrator may not be used in its role as Plan Sponsor. Procedures must be put in place to assure this separation between the health plan and the Plan Sponsor. Such procedures are attached as **Exhibit D**. The employer will be required to certify to the Plan Administrator in writing that, as Plan Sponsor, it has complied with these provisions and that the plan documents have been appropriately amended. Of course, if the employer serves as both Plan Sponsor and Plan Administrator, it will be providing a certification to itself.

⁴ "Plan administration" activities are limited to activities that would meet the definition of payment or health care operations, but do not include functions to modify, amend or terminate the plan or solicit bids from prospective issuers. Plan administration functions include quality assurance, claims processing, auditing, monitoring and management of carve-out plans, such as vision and dental. It does not include any employment-related functions or functions in connection with any other benefits or benefit plans.

Options for dealing with the Plan Sponsor's need for PHI:

1. When the Privacy Standards take effect in April of 2003, ask all existing participants for the needed authorizations and subsequently ask new participants for authorizations at the time of enrollment. Authorizations should enable the Plan Sponsor to receive PHI and disclose it to stop-loss carriers for underwriting purposes (recall that underwriting is a health care operation within the definition of TPO), and to use PHI for employment-related purposes, such as sharing with other plans, and purposes relating to the Family and Medical Leave Act or the Americans With Disabilities Act.
2. The Plan Sponsor may ask the Plan Administrator to disclose PHI to stop-loss carriers for underwriting purposes on behalf of the Plan Sponsor to enable the Plan Sponsor to obtain insurance coverage for the plan, and no authorization is needed. The Plan Sponsor then seeks authorizations, as needed, from individuals to use and/or disclose PHI for employment-related purposes.

Because under option 1 above, plans can condition enrollment for new employees on supplying authorizations but cannot do so for existing employees (and thus, cannot force existing employees to give an authorization) and, in light of the massive amount of paper work involved in obtaining all of the authorizations required by option 1, **we suggest using option 2.** (Again, see Item 5 in the section entitled "Use and Disclosure of Protected Health Information In General", setting forth the circumstances under which a plan may condition enrollment and eligibility for benefits upon receipt of an authorization.) We are addressing option 2 in plan amendments. However, we are providing an authorization that can be used under either option.

In addition, the plan may disclose Summary Health Information to the Plan Sponsor if the Plan Sponsor requests it for the purpose of (a) obtaining premium bids from health plans for providing health insurance coverage under the group health plan, or (b) modifying, amending or terminating the group health plan. Plan documents need not be amended to enable disclosure of Summary Health Information in these situations. "*Summary Health Information*" may be individually identifiable health information and it summarizes the claims history, claims expenses or the type of claims experienced by individuals in the plan, but it excludes all identifiers that must be removed for the information to be de-identified, except that it may contain geographic information to the extent that it is aggregated by five-digit zip code.

Further, without the need to amend plan documents, the Privacy Standards indicate that a plan may disclose to the Plan Sponsor information on whether the individual is participating in the plan, or is enrolled in or has disenrolled from the plan.

B. The Employer as the Plan Administrator

When the employer is acting as the Plan Administrator, it is responsible for all of the operations and administration of the plan, unless the plan documents allocate certain responsibilities to other fiduciaries. As the Plan Administrator, the employer is a fiduciary and must act in the best interests of all the plan's participants. Of course, it has the liability associated with fiduciary status. Technically, the Plan Administrator is not a Covered Entity; rather, the Covered Entity is the plan itself. However, the plan is nothing more than its plan document and summary plan description and perhaps a bank account. Its actions are taken by the Plan Administrator, which, practically speaking, makes the Plan Administrator a Covered Entity.

As the Plan Administrator, the employer has full access to PHI; it is permitted to use the PHI for TPO purposes, but it is not permitted to use it for employment-related decisions, such as hiring, firing or promotions, and must have appropriate procedures in place to prevent such use. Such procedures are attached as **Exhibit D**. However, it is important to consider how much PHI should be disclosed and used by the individual designated as the plan's named fiduciary for purposes of making a decision regarding an appeal of a denial of benefits on behalf of the Plan Administrator (which usually is the employer). As always, only the minimum necessary information may be used by, and disclosed to, the individual fiduciary. On the other hand, the plan must be certain that the individual fiduciary has the necessary PHI to decide an appeal.

2. How do the Privacy Standards apply to disclosures to plan participants?

The Privacy Standards permit the use and disclosure to an individual plan participant of that individual's own PHI. There is no requirement for consent or authorization. Also, the "minimum necessary" requirement does not apply to disclosures to individuals.

3. How do the Privacy Standards apply to disclosures to family members of participants?

A Covered Entity, without consent or authorization, may disclose to a family member or other relative PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's health care, as follows:

If the individual is present for, or otherwise available prior to, such use or disclosure and has the capacity to make health care decisions, the Covered Entity may use or disclose the PHI if it

- obtains the individual's agreement;
- provides the individual the opportunity to object to the disclosure and the individual fails to do so; or
- reasonably infers from the circumstances, based upon the exercise of professional judgment, that the individual does not object to the disclosure.

Note that the Covered Entity may orally inform the individual of, and obtain the individual's oral agreement or objection to, a use or disclosure.

Additionally, if the individual is not present, or the opportunity to agree or object to the use or disclosure cannot be provided because of the individual's incapacity or an emergency circumstance, the Covered Entity may, in the exercise of professional judgment, determine if the disclosure is in the best interest of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's health care.

Plans must verify that the family member is involved in the individual's care or in paying for that care. The Privacy Standards do not address how this is to be done. Plan Administrators must use professional judgment and experience with common practice. For example, if an individual brings a spouse to an appeal hearing regarding a denied claim for benefits, or if a spouse, on behalf of the individual participant, submits a letter of appeal, PHI may be disclosed to the spouse to the extent the PHI is relevant to the claim in question.

Because a parent usually has authority to make health care decisions about his or her minor child, a parent generally is a "personal representative" of that minor child under the Privacy Standards and has the right to obtain access to health information about the minor child. There are exceptions in which a parent might not be the "personal representative" with respect to certain health information about a minor child. In the following situations, the Privacy Standards defer to determinations under other law that the parent does not control the minor's health care decisions and, thus, does not control the PHI related to that care: (1) when a state or other law does not require consent of a parent or other person before a minor can obtain a particular health care service, and the minor consents to the service, the parent is not the minor's personal representative unless the minor has requested that the parent be treated as the personal representative; (2) when the minor may lawfully obtain health care services without the consent of a parent, and the minor, a court or another person authorized by law consents to such health care service, the parent is not the personal representative of the minor for the relevant services; (3) when a parent agrees to a confidential relationship between the minor and the physician, the parent does not have access to the health information related to that relationship; and (4) when a Covered Entity reasonably believes in its professional judgment that the child has been or may be subject to abuse or neglect, or that treating the parent as the child's personal representative could endanger the child, the Covered Entity may choose not to treat the parent as the personal representative of the child. Despite the provisions set forth in exceptions 1-3 above, the Privacy Standards provide that:

- If, and to the extent, permitted or required by an applicable provision of state or other law, including applicable case law, a Covered Entity may disclose, or provide access to, PHI about a minor to a parent;
- If, and to the extent, prohibited by an applicable provision of state or other law, including applicable case law, a Covered Entity may not disclose, or provide access to, PHI about a minor to a parent; and
- Where a parent is not the personal representative as detailed in exceptions 1-3 above and where there is no applicable access provision under state or other law, including case law, a Covered Entity may provide or deny access to a parent if such action is consistent with state or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

4. How do the Privacy Standards apply to disclosures to representatives of participants?

A Covered Entity must, with certain exceptions, treat a personal representative as the individual for purposes of the Privacy Standards. Thus, a plan may disclose PHI to a personal representative without consent or authorization, and the "minimum necessary" requirements do not apply to such disclosures unless the purpose for which the personal representative was appointed is limited. If the purpose of representation is limited, only PHI relating to the limited purpose of the representation may be disclosed, but PHI unrelated to the limited purpose of the representation cannot be disclosed. (For example, if a personal representative is appointed for the limited purpose of making decisions regarding an individual's cancer treatment, PHI unrelated to that individual's cancer treatment cannot be disclosed to the personal representative.) The plan must verify the identity and the authority of the individual claiming to be a personal representative before making any disclosure of PHI.

If under applicable law, a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a Covered Entity must treat such person as a personal representative. Also, if under applicable law, an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a Covered Entity must treat such person as a personal representative with respect to PHI relevant to such representation. If under applicable law, a parent, guardian or other person acting *in loco parentis* has authority to act on behalf of

an individual who is an unemancipated minor in making decisions related to health care, a Covered Entity must treat such person as a personal representative. However, see Item 3 above regarding exceptions and further details about treating a parent as a minor's personal representative. A Covered Entity may elect not to treat a person as the personal representative of an individual if (a) it has a reasonable belief that the individual has been or may be subjected to domestic violence, abuse or neglect by such person or that treating such person as the personal representative could endanger the individual, and (b) the Covered Entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

Another issue that must be addressed is how the "authorized representative" provisions of ERISA's new claims processing regulations (the "Claims Regulations") affect the "personal representative" provisions of the Privacy Standards. The Claims Regulations do not define an authorized representative, but they require a plan to permit an individual to designate an authorized representative to act on their behalf. (If a claim involves urgent care, the plan must, without regard to its procedures for the designation of an authorized representative, permit a health care professional with knowledge of the individual's medical condition, such as a treating physician, to act as the individual's authorized representative.) As indicated above, the Privacy Standards require plans to recognize a person as a personal representative in certain situations. It is believed that the Claims Regulations would be considered "applicable law" providing adequate legal authority for individuals designated under those regulations to act as personal representatives under the Privacy Standards. Attached as **Exhibit E** is a form for use by a plan when a participant wishes to designate an authorized representative. You will note that it includes a notice that the authorized representative may become aware of PHI.

5. How do the Privacy Standards apply to disclosures to medical providers?

The "minimum necessary" requirement regarding disclosures of PHI does not apply to disclosures to a provider for treatment. Keep in mind, however, that treatment generally does not relate to the activities of plans. Nonetheless, plans may disclose PHI without consent to carry out TPO purposes. Presumably, any disclosure to a provider would fall within either the payment or health care operations elements of TPO. These disclosures will be governed by the "minimum necessary" requirement. If a disclosure to a provider is not for TPO purposes, the plan will need to obtain an individual's authorization to make that disclosure.

6. How do the Privacy Standards apply to disclosures to MGUs and stop-loss carriers?

The Privacy Standards do not address whether managing general underwriters ("MGUs") and stop-loss carriers are Business Associates, and there is much debate on this issue. The cause for the debate is the fact that stop-loss policies are generally issued to employers, as Plan Sponsors, who are not Covered Entities and, therefore, cannot have Business Associates. However, we do not believe that the analysis should stop there, or that courts will do so if the question arises. Rather, we believe that the courts will ignore this fine distinction (and, in fact, they have already done so in the context of whether or not a stop-loss policy is a plan asset) and find that MGUs and carriers are Business Associates. Accordingly, we recommend that a Business Associate Agreement be put in place with these entities.

As far as whether use and disclosure of PHI by MGUs and carriers falls under the definition of TPO, it would appear that it does and that a consent or authorization will not be necessary. However, if information is needed by one of these entities from a health care provider for underwriting purposes, the

provider must obtain an authorization to disclose such information because underwriting is not a health care operation of the provider and the disclosure is not otherwise permitted.

If it will be the employer, as Plan Sponsor, who is initially disclosing PHI to MGUs and carriers, an authorization must be obtained from each participant relating to the Plan Sponsor's use of PHI, covering any necessary disclosures to MGUs and carriers (as outlined in option 1 in Item 1A above). However, if the Plan Sponsor directs the Plan Administrator to disclose PHI to MGUs and carriers on behalf of the Plan Sponsor, authorizations from all participants will not be required (as outlined in option 2 in Item 1A above).

As always, when disclosing PHI to MGUs and carriers, a plan must make reasonable efforts to limit the PHI to the minimum necessary to accomplish the intended purpose of the disclosure. The plan must ensure that it does not disclose an individual's entire medical record, even for TPO purposes, unless the disclosure of the entire record is specifically justified. If the plan receives a request for an individual's entire medical record, the plan must require the requesting party to justify that request.

7. *How do the Privacy Standards apply to disclosures to other third-party vendors, such as PPOs, utilization review companies, prescription drug vendors, etc.?*

To answer this, it first must be determined (a) if the vendor is a Business Associate of the plan and (b) what is the purpose of the disclosure. As indicated previously, Business Associates essentially perform, on behalf of Covered Entities, or assist Covered Entities in performing, various functions such as legal services, utilization review, quality assurance, and benefit management. Thus, the functions of most third-party vendors appear to fall within the definition of Business Associate. However, when examining if the vendor is a Business Associate of the plan, you must examine how the relationship is set up. If the relationship is a direct one between the plan and the vendor, *i.e.*, there is a contract between the plan and the vendor (assuming the vendor performs a function falling within the definition of Business Associate), then the plan will need to enter into a Business Associate Agreement with the vendor. Business Associate Agreements are discussed in more detail in the section entitled "Health Plan Compliance with the Privacy Standards." A form of Business Associate Agreement is attached as **Exhibit F**. On the other hand, if the relationship is an indirect one between the plan and the vendor, *i.e.*, the contract is between the TPA and the vendor enabling the plan to take advantage of the vendor's services, the TPA will need to enter into a Subcontractor/Agent Agreement with the vendor.

As discussed above, plans may disclose PHI without consent or authorization to carry out TPO purposes. Further, in essence, plans may only disclose PHI to a Business Associate in accordance with a Business Associate Agreement that limits the use and disclosure of PHI under the same restrictions that apply to the plan. Thus, assuming the vendor is a Business Associate of the plan, if the disclosure is made directly to the third-party vendor for TPO purposes, no consent or authorization is needed. The vendor will be expected to comply with restrictions on its use and disclosure of the PHI consistent with the Privacy Standards and its Business Associate Agreement. Alternatively, assuming the vendor is a subcontractor or agent of the TPA, if the disclosure is made to the TPA for TPO purposes, who in turn discloses the PHI to the vendor (also, for TPO purposes), still no consent or authorization is needed. The TPA will be expected to comply with the restrictions on its use and disclosure of the PHI consistent with the Privacy Standards and its Business Associate Agreement with the plan; via that Business Associate Agreement, the TPA has agreed to ensure that its subcontractors/agents—the vendor in this case—agree to the same restrictions on use and disclosure of PHI consistent with the Privacy Standards. Thus, in turn, the vendor will be expected to comply with the restrictions on its use and disclosure of the PHI consistent with the Privacy Standards and its Subcontractor/Agent Agreement with the TPA. Finally, again assuming the vendor is a subcontractor or agent of the TPA, but the disclosure is made directly to the vendor for TPO

purposes (bypassing the TPA), no consent or authorization is needed. The vendor will be expected to comply with the restrictions on its use and disclosure of the PHI consistent with the Privacy Standards and its Subcontractor/Agent Agreement with the TPA from which the plan indirectly benefits. (As indicated, the TPA, via its Business Associate Agreement with the plan, has agreed to ensure that its subcontractors/agents—the vendor in this case—agree to the same restrictions on use and disclosure of PHI consistent with the Privacy Standards.)

Further, if the disclosure is for a purpose other than TPO, the plan will need to obtain the individual's authorization to disclose PHI to the vendor. Keep in mind that, among other things, the authorization will need to identify the vendor (and possibly the TPA, if there is an indirect relationship) as a recipient of the disclosed PHI. De-identified information always can be disclosed because it is not subject to the protections of the Privacy Standards. Additionally, the plan can disclose a Limited Data Set if the disclosure is for purposes of health care operations as long as it enters into a Data Set Agreement with the recipient of the Limited Data Set. Data Set Agreements are discussed in more detail in the section entitled "HIPAA's Privacy Standards in General."

8. How do the Privacy Standards apply to disclosures to a TPA's advisors, such as attorneys?

Like the previous question, to answer this it first must be determined (a) if the advisor is a Business Associate of the plan and (b) what is the purpose of the disclosure. You will recall that Business Associates may perform legal services on behalf of Covered Entities. Thus, an attorney appears to fall within the definition of Business Associate. However, when examining if a TPA's attorney advisor is a Business Associate of the plan, you again must examine how the relationship is set up. If the relationship is a direct one between the plan and the attorney advisor, *i.e.*, the attorney provides legal services and advice directly to the plan, then the plan will need to enter into a Business Associate Agreement with the attorney advisor. Business Associate Agreements are discussed in more detail in the section entitled "Health Plan Compliance with the Privacy Standards." A form of Business Associate Agreement is attached as **Exhibit F**. On the other hand, if the attorney provides legal services and advice to the TPA relating to services performed for the plan⁵ (for example, after reviewing a plan document to determine if a claim is covered by the plan, an attorney advises the TPA as to this determination, and, based upon this advice, the TPA makes a recommendation to the Plan Administrator that the claim should be paid) then there is an indirect relationship between the plan and the attorney and the TPA will need to enter into a Subcontractor/Agent Agreement with the attorney.

Once again, plans may disclose PHI without consent or authorization to carry out TPO purposes. Additionally, generally plans may only disclose PHI to a Business Associate in accordance with a Business Associate Agreement that limits the use and disclosure of PHI under the same restrictions that apply to the plan. Thus, assuming the attorney advisor is a Business Associate of the plan, if the disclosure is made directly to the attorney for TPO purposes, no consent or authorization is needed. The attorney will be expected to comply with restrictions on its use and disclosure of the PHI consistent with the Privacy Standards and its Business Associate Agreement. Alternatively, assuming the attorney is a subcontractor or agent of the TPA, if the disclosure is made to the TPA for TPO purposes, who in turn discloses the PHI to the attorney (also, for TPO purposes), still no consent or authorization is needed. The TPA will be expected to comply with the restrictions on its use and disclosure of the PHI consistent with the Privacy Standards and its Business Associate Agreement with the plan; via that Business

⁵ We need not address those situations when an attorney provides legal services to the TPA that are unrelated to services that the TPA performs on behalf of the plan and, instead, related to the TPA's own business concerns (such as advising the TPA regarding negotiating an unrelated contract or providing tax advice to the TPA), because there clearly is no need to disclose PHI to the attorney in such cases.

Associate Agreement, the TPA has agreed to ensure that its subcontractors/agents—the attorney in this case—agree to the same restrictions on use and disclosure of PHI consistent with the Privacy Standards. Thus, in turn, the attorney will be expected to comply with the restrictions on its use and disclosure of the PHI consistent with the Privacy Standards and its Subcontractor/Agent Agreement with the TPA. Note that, unlike in the prior question where we assumed that there are cases in which a vendor could be a subcontractor of the TPA but a disclosure of TPO could be made directly to the vendor bypassing the TPA, we do not believe that such a situation is applicable to an attorney advisor. When a plan, seeking legal advice, directly discloses PHI to an attorney, the attorney would have an ethical duty, pursuant to the Rules of Professional Conduct, to establish an attorney-client relationship with the plan, in which case the attorney would become a Business Associate of the plan.

Finally, if the disclosure is for a purpose other than TPO, the plan will need to obtain the individual's authorization to disclose PHI to the attorney. Keep in mind that, among other things, the authorization will need to identify the attorney (and possibly the TPA, if there is an indirect relationship) as a recipient of the disclosed PHI. De-identified information always can be disclosed because it is not subject to the protections of the Privacy Standards. Additionally, the plan can disclose a Limited Data Set if the disclosure is for purposes of health care operations as long as it enters into a Data Set Agreement with the recipient of the Limited Data Set. Data Set Agreements are discussed in more detail in the section entitled "HIPAA's Privacy Standards in General."

9. *Does the plan have a duty to verify the identity of an individual or entity requesting PHI before disclosure?*

Yes. Prior to disclosing PHI, a Covered Entity, except in certain limited circumstances, must verify the identity of the person requesting PHI and the authority of that person to have access to PHI if the identity or authority of the person is not known to the Covered Entity. In addition, the Covered Entity must obtain any documentation, statements, or representations, whether oral or written, from the person requesting the PHI when the documentation, statements, or representations are required under the Privacy Standards. By virtue of its Business Associate Agreement, the TPA also will be required to obtain such verification prior to disclosing PHI. Accordingly, plans and TPAs will need to adopt verification procedures to review a person's identification and authority to access PHI. Consents, authorizations, proof of personal representation, powers of attorney and other appropriate documentation must be obtained prior to disclosing PHI. Suggested procedures also may include requesting a provider's employer identification number (EIN) to verify identity when a provider requests PHI or requesting a participant's social security number (assuming state law permits this) to verify the participant's identity when the participant requests PHI. Suggested verification procedures are attached as **Exhibit G**.

A plan may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, appear valid. Therefore, there is no need to double-check the documentation. With regard to identity, a plan may rely, if reasonable under the circumstances, on any of the following to verify identity of a public official when disclosing PHI to a public official or person acting on behalf of the public official:

- If the request is made in person, presentation of an agency identification badge, other official credential, or other proof of government status;
- If the request is in writing, the request is on the appropriate government letterhead; or
- If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under government authority or other

evidence or documentation of agency that establishes that the person is acting on behalf of the public official.

With respect to authority, a plan may rely, if reasonable under the circumstances, on any of the following to verify authority of a public official when disclosing PHI to a public official or person acting on behalf of the public official:

- A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority; or
- If a request is made pursuant to legal process, a warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

As discussed in Item 3 above, plans may rely on professional judgment and experience with common practice to verify that a family member is involved in an individual's care or in paying for that care to allow disclosure of PHI to that family member.

Health Plan Compliance with the Privacy Standards

To comply with the Privacy Standards, a plan should take the following actions. Preliminarily, we suggest that you first consult with your TPA so that you can coordinate your compliance efforts with your TPA and avoid duplicative efforts.

1. Enter into Business Associate Agreements with each Business Associate.

(It is mandatory that the TPA and any other Business Associate sign a Business Associate Agreement with the plan.) A form of Business Associate Agreement is attached as **Exhibit F**.

Preliminarily, the Business Associate Agreement is between a Covered Entity (the plan) and a Business Associate (for example, a TPA). An employer is not a Covered Entity and, therefore, is not a party to the Business Associate Agreement. Instead, a Plan Administrator enters into the contract on behalf of the plan (that is, the employer, acting in its capacity as Plan Administrator, enters into the contract).

The Business Associate Agreement must do the following:

- Establish the permitted and required PHI uses and disclosures by the Business Associate;
- Prevent the Business Associate from any further use or disclosure which would violate the Privacy Standards, the Agreement itself, or other applicable law;
- Authorize the Covered Entity to terminate the contract if the Business Associate violates a material term;
- Require that the Business Associate use appropriate safeguards to prevent PHI use or disclosure other than as provided for in the contract;
- Require the Business Associate to report to the Covered Entity any unauthorized use or disclosure;
- Require that the Business Associate ensure its agents or subcontractors that receive PHI from it agree to the same restrictions and conditions;
- Make PHI available based upon the Privacy Standards' requirements regarding individuals' right to access their PHI;
- Make PHI available for amendment and incorporate any amendments in accordance with the Privacy Standards;
- Make available the information required to provide an accounting of disclosures of PHI;
- Make the Business Associate's internal practices, books and records relating to PHI available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining compliance; and
- Require that, at contract termination, the Business Associate will return or destroy all PHI, or, if not feasible, extend the protections of the contract to the PHI that it continues to maintain and limit further use or disclosure of the PHI.

It may do the following:

- Permit the Business Associate, if necessary, to use and disclose PHI for its proper management and administration or to carry out its legal responsibilities;
- Permit the Business Associate to provide data aggregation services; and

- Address de-identification of PHI.

Additionally, because the Privacy Standards do not contain a private right to sue for violations, we recommend that Business Associate Agreements also contain a provision expressly stating that there are no third party beneficiaries of the agreements. This may eliminate a "back door" lawsuit by individual participants attempting to sue for violations under the Business Associate Agreement as third party beneficiaries to those agreements.

A Covered Entity may incur liability under the Privacy Standards if it knew of a pattern of activity or practice of its Business Associate that constituted a material breach of the Business Associate's obligation under the Business Associate Agreement unless the Covered Entity took reasonable steps to cure the breach, and, if such steps were unsuccessful:

- Terminated the Business Associate Agreement; or
- If termination was not feasible, reported the problem to the Secretary of HHS.

Therefore, a plan may be liable, under certain circumstances, if a Business Associate violates its Business Associate Agreement when the plan knew of the violation.

The deadline for entering into Business Associate Agreements has been extended until April 14, 2004 unless the Business Associate's existing service agreement with the plan is renewed or modified between October 15, 2002, and April 14, 2003. If the existing service agreement is renewed or modified in this interim time period, the plan and Business Associate must enter into a Business Associate Agreement on the date the existing service agreement is renewed or modified.

Attached as **Exhibit F** is a form of Business Associate Agreement for your use. Again, however, we advise that you consult with your TPA before utilizing this form.

2. Obtain any authorizations that may be needed.

Health plans may use PHI for TPO purposes without consent or authorization. See Item 5 in the section entitled "Use and Disclosure of Protected Health Information in General" and Item 1A in the section entitled "Use and Disclosure of Protected Health Information in Specific Situations" for a detailed discussion of authorizations. A form of authorization is attached as **Exhibit A**.

3. Amend the Plan Document and Summary Plan Description.

Amend your plan documents to provide for adequate separation between the plan and Plan Sponsor, to establish the permitted and required uses and disclosures of PHI by the Plan Sponsor and, possibly, to condition coverage upon the participant's authorization for certain uses and disclosures of PHI or, alternatively, to authorize the Plan Administrator to provide PHI to stop-loss carriers on behalf of the Plan Sponsor. (Note, however, that such authorizations must be obtained prior to enrollment if the plan will condition coverage upon providing the authorization.) A general form of amendment is attached as **Exhibit B**.

4. Adopt procedures to comply with the "minimum necessary" requirements.

A plan's use or disclosure of, or requests for, PHI must consist of only the minimum amount necessary to accomplish the intended purpose of the use, disclosure or request. Initially, before identifying the minimum necessary PHI required, start by determining if the intended purpose of the use, disclosure or request for disclosure of PHI could be satisfied by using de-identified information. If so, the Privacy Standards do not apply and there is no need to assess the minimum necessary PHI required.

With respect to the minimum necessary uses of PHI, plans must:

- Identify those persons or classes of persons, as appropriate, in your workforce who need access to PHI to carry out their duties;
- For each such person or class of persons, identify the category or categories of PHI to which access is needed and any conditions appropriate to such access; and
- Make reasonable efforts to limit the access of those persons or classes identified to the category of PHI to which access is needed.

With respect to the minimum necessary disclosure of PHI, plans must:

- For disclosures made on a routine and recurring basis, implement policies and procedures that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure; and
- For all other disclosures, develop criteria designed to limit PHI disclosed to information reasonably necessary to accomplish the purpose for which disclosure is sought, and review requests for disclosure on an individual basis in accordance with those criteria.

The plan can rely, if reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose(s) when:

- Making disclosures to public officials that are permitted by the Privacy Standards if the public official represents that the information requested is the minimum necessary for the stated purpose(s);
- The information is requested by a Covered Entity;
- The information is requested by a professional who is a member of the plan's workforce, or is a Business Associate of the plan, for the purpose of providing professional services to the plan, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or
- Documentation or representations that comply with the requirements of the Privacy Standards have been provided by a person requesting the information for research purposes. We did not describe the requirements of the Privacy Standards with respect to proper documentation or representations needed regarding information for research purposes because we believe this will be inapplicable to plans.

With respect to minimum necessary requests for PHI, plans must:

- Limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made when requesting PHI from Covered Entities;
- For requests made on a routine and recurring basis, implement policies and procedures that limit PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made; and

- For all other requests, develop criteria designed to limit the request for PHI to the information reasonably necessary to accomplish the purpose for which the request is made, and review requests for disclosure on an individual basis in accordance with such criteria.

Keep in mind, the Privacy Standards expressly state that use, disclosures or requests for an entire medical record are prohibited unless the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request. If large amounts of PHI or entire medical records are specifically justified as reasonably necessary to conduct aggregate audits, this is permissible under minimum necessary.

HHS has stressed that it contemplates that Covered Entities will establish reasonable policies and make reasonable efforts to limit disclosure of PHI, while still having the flexibility they need for their operations. The policies and procedures adopted are important, since the Privacy Standards permit them to take the place of a case-by-case examination of all routine disclosures of, and requests for, PHI. Case-by-case analysis is only required for non-routine disclosures or requests. Recommended procedures for Plan Administrators are attached as **Exhibit H**.

Importantly, the minimum necessary requirements do not apply to:

- Disclosures to or requests by a health care provider for treatment;
- Uses or disclosures made to the individual—note that this also would cover uses or disclosures made to an individual's personal representative as long as that use or disclosure is within the purpose of the representation if representation is limited to a particular purpose;
- Uses or disclosures pursuant to an authorization;
- Disclosures made to the Secretary of HHS in accordance with the Privacy Standards;
- Uses or disclosures that are required by law; and
- Uses or disclosures that are required for compliance with the Privacy Standards or EDI Transaction Standards. However, with regard to EDI Transaction Standards, only required data elements are exempt from minimum necessary requirements. Minimum necessary requirements apply to the use of optional data elements.

Remember, disclosures to the employer, when acting in its capacity as the Plan Sponsor, always are subject to the minimum necessary requirements.

5. Establish firewalls; limit employees with access to PHI.

Establish safeguards or "firewalls" to prevent access to PHI by employees who are not involved in health plan operations. You also will need to safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure. The access controls discussed above that determine who can access and use PHI are essential elements of a firewall. Basically, the plan will need to appoint one or more employees (or positions, such as "Human Resource Manager, or classes of employees) to receive, use and safeguard PHI (during enrollment, claims processing and appeals). Alternatively, it may be easier to designate the individuals who are not involved and have no need to access PHI. Each individual with PHI access should be trained to understand the importance of his or her role and to assure that he or she does not disclose PHI to any other employees or for any purpose other than those related to the plan. If possible, a person with access to PHI should not be responsible for employment-related decisions, such as hiring, promotions or terminations, or for any other benefit plan, so that PHI is used only for administration of the health plan and not for any other purpose (for example, it cannot be used in connection with a separate short-term disability plan unless appropriate authorizations

have been obtained to permit this). Further, the plan must examine its offices to determine if any physical changes are needed to safeguard PHI. For example, is the fax machine located in an area where only the appropriate personnel can access it? Are paper records protected from inspection by unauthorized individuals? Attached as **Exhibit I** is a checklist of items for employers to consider.

After the Security Standards are finalized, implementation of those standards will assist in securing PHI by requiring certain access controls.

6. *Designate a privacy official.*

Designate a "privacy official" who will be responsible for the development and implementation of policies and procedures regarding uses, disclosures, and requests for PHI, including a process for individuals to lodge complaints. The following is a list of the privacy official's key duties and responsibilities:

- Track all PHI, including recording all uses and disclosures and requests for PHI by the plan, from the plan to vendors and from the plan to any other third party. Determine what employees have access to PHI and for what reasons. A form for tracking PHI uses, disclosures and requests is attached as **Exhibit J**.
- Make sure legal documentation is in place, such as plan document amendments, Business Associate Agreements, and authorizations.
- Coordinate compliance with the Privacy Standards with related laws and regulations, including ERISA (as well as its Claims Regulations), EDI Transaction Standards and Security Standards (when finalized). Coordinate uses and disclosures with other functions, such as for employment-related purposes or a companion pension or disability plan. It will be necessary to determine how many plans an employer maintains. For example, does it have a medical plan and a separate dental plan, with separate Form 5500s? The answer to this will affect the ability to use and disclose information.
- Set up structures to ensure individuals' rights, which will involve a process for plan participants to request access to their PHI. Establish procedures for when plan participants may inspect, copy, amend or request restrictions on disclosure of their PHI, as well as procedures to track disclosures and accounting requests and ensure that written accountings are provided within the required timeframes.⁶ Processes must be put in place to document the implementation of these rights. Appropriate guidelines and forms are attached as **Exhibit K**.
- Set up a complaint process and sanctions for employees found violating the policies and procedures and improperly using, disclosing, or requesting PHI, and implement procedures for resolution of complaints and to mitigate resulting damages. Suggested guidelines are attached as **Exhibit L**.
- Adopt privacy policies and procedures, which document all of the areas the privacy official oversees, including how PHI is used and disclosed, individual rights and the complaint process, and how PHI is destroyed or maintained when no longer needed.

⁶ While an individual has a right to receive an accounting of disclosures of PHI made in the six years prior to the date on which an accounting is requested, this right does not apply to disclosures: (1) to carry out treatment, payment and health care operations; (2) to individuals themselves; (3) incident to a use or disclosure otherwise permitted or required by the Privacy Standards; (4) pursuant to an authorization; (5) to persons involved in the individual's care consistent with the Privacy Standards; (6) for national security or intelligence purposes; (7) to correctional institutions or law enforcement officials having custody of the individual; (8) as part of a Limited Data Set in accordance with the Privacy Standards; or (9) that occurred prior to the compliance date (April 14, 2003).

Ensure that such policies and procedures are followed. Develop the Notice of Privacy Practices, which is required to be provided to participants. A suggested form of Notice of Privacy Practices is attached as **Exhibit M**.

- Develop a training program for any individuals supervised by the privacy official and for any employees who have access to PHI.
- Audit and monitor to ensure compliance with the Privacy Standards and that internal policies and procedures regarding PHI are followed.
- Keep up-to-date regarding the latest privacy developments and ensure legal compliance with any changes.

All referenced policies or procedures should be maintained in written or electronic form and retained for six years from the date of its creation or the date when last in effect, whichever is later.

Attached as **Exhibit N** are suggested policies and procedures.

7. Designate a contact person for complaints and notices.

Designate a contact person (or position) for receiving complaints, providing the Notice of Privacy Practices required by the Privacy Standards and providing additional information regarding the Notice. This contact person may be, but need not be, the same person as the privacy official. If they are not the same person, then the contact person should report to the privacy official regarding his or her duties as such. A suggested form of Notice of Privacy Practices is attached as **Exhibit M**.

8. Institute procedures for resolving, and sanctions for, improper use or disclosure.

Institute a procedure for resolving any issues of non-compliance with the Privacy Standards; mitigate, to the extent practicable, any harmful effect that is known to the plan resulting from an improper use or disclosure; and design a system of sanctions for employees who violate the rules. Make employees aware that violations of privacy policies and procedures will not be taken lightly. Sanctions may include written warning, loss of privileges or termination in repeated and/or extreme cases. Progressive discipline for violations is recommended. Further, plans must make employees aware of potential sanctions by publishing them in employment policies and procedures. Suggested guidelines are attached as **Exhibit L**.

9. Comply with participants' rights regarding PHI.

As indicated previously, plans must make PHI in a designated record set available to plan participants for inspection and copying. A designated record set consists of the enrollment, payment, claims adjudication and case or medical management record systems maintained for the plan, or a group of records used, in whole or in part, by or for the plan to make decisions about individuals. Plans must decide what makes up the designated record set, document that determination and establish procedures for handling requests for access. Importantly, the right to inspect and copy PHI excludes psychotherapy notes and information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding. Additionally, plans must consider individual's requests for amendments to PHI, and, upon request, provide them with an accounting of PHI disclosures. Appropriate guidelines and forms are attached as **Exhibit K**.

10. Respond to requests by HHS.

Make your internal practices and records relating to the use and disclosure of PHI available to HHS upon request.

11. Institute procedures for destruction or maintenance of PHI.

Under the Privacy Standards, when PHI is no longer needed, destroy it or maintain it in a manner that limits its use or disclosure.

You may wish to consider the following:

- Shredding documents that can be destroyed consistent with the Privacy Standards if there is no possibility that those documents may be needed for litigation defense or other purposes; or
- Marking records that contain PHI prior to storage of those records so that employees are aware that PHI contained in those records is still subject to the Privacy Standards and your internal policies and procedures regarding restrictions on use and disclosure.

12. Certify compliance.

Certify that it has taken certain required actions to comply with the Privacy Standards. A form of certificate is attached as **Exhibit C**.

13. Distribute the Notice of Privacy Practices.

The plan must distribute the Notice of Privacy Practices to all individuals covered by the plan. Thereafter, at the time of enrollment, it must distribute the Notice to new enrollees. Further, within 60 days of a material revision to the Notice, it must distribute it to individuals then covered by the plan. Also, no less frequently than once every three years, the plan must notify individuals covered by the plan of the availability of the Notice and how to obtain it.

A form Notice of Privacy Practices is attached as **Exhibit M**.

Other Operational Issues

1. Do the HIPAA regulations conflict with the U.S. Department of Labor's new Claims Regulations? If so, how do we handle those conflicts?

The Claims Regulations and the Privacy Standards intersect in various ways:

- Time limits. The Claims Regulations mandate that benefits claims and appeals be addressed within certain time limits that are designed to accelerate the processing of claims and appeals. Nevertheless, the Privacy Standards must be satisfied. Accordingly, plans must implement policies and procedures regarding the Privacy Standards and thoroughly train employees regarding both the Claims Regulations and the Privacy Standards. This must be done to avoid any unintentional uses and/or disclosures of PHI that may result from efforts to comply with the accelerated processing time limits.
- Interaction of the "relevant" definition of the Claims Regulations with minimum necessary requirements. Under the new Claims Regulations, an individual must be provided copies of all information "relevant" to their claim for benefits.

"Relevant" information is broadly defined and includes documents, records and information if: (a) it was relied upon in making the benefit determination; (b) it was submitted, considered or generated in the course of the benefit determination, whether or not it was relied upon; (c) it demonstrates compliance with the requirements of the new regulations that claim determinations are made in accordance with plan documents and that, where appropriate, the plan provisions have been applied consistently with respect to similarly situated claimants; or (d) it constitutes a statement of policy or guidance with respect to the plan concerning the denied benefit for the claimant's diagnosis, whether or not it was relied upon.

The Privacy Standards require that only the minimum necessary information to determine the claim or appeal be disclosed. Technically, information and data from other claimants' files may fall under the Claims Regulations' definition of "relevant information." However, the Department of Labor has indicated that a plan is not required to disclose that information. Therefore, the definition of relevant information does not appear to conflict with the minimum necessary requirements. Still, plans will have to examine whether requests for relevant information regarding a claim constitute routine or non-routine disclosures and develop policies and procedures to address such disclosures.

- "Authorized representative" provisions of the Claims Regulations compared to the "personal representative" provisions of the Privacy Standards. It is believed that the Claims Regulations would be considered "applicable law" providing adequate legal authority for individuals designated under those regulations to act as personal representatives under the Privacy Standards. See Item 4 in the section entitled "Use and Disclosure of Protected Health Information in Specific Situations" for a detailed discussion of this comparison.
- Disclosure of PHI to an individual designated as the plan's named fiduciary for purposes of deciding claims appeals on behalf of the Plan Administrator (usually, the employer). Only the minimum necessary information may be used by, and disclosed to, the individual fiduciary.

However, the plan must be certain that the individual fiduciary has the necessary PHI to decide an appeal.

- Consistency requirement of the Claims Regulations. The Claims Regulations mandate that plan provisions be applied consistently with regard to similarly situated claimants. As indicated above, information and data from other claimants' files may be useful in demonstrating this consistency. Presumably, the plan can review the files of other claimants to demonstrate consistency without consent because it relates to payment purposes, provided it reviews only the minimum necessary PHI to determine if plan provisions were applied consistently. Again, however, the Department of Labor has indicated that a plan is not required to disclose that information to individuals.
- Medical consultation required by Claims Regulations. The Claims Regulations require that when a decision is based upon a medical judgment (such as whether the treatment is medically necessary or is experimental), the fiduciary shall consult with an appropriate health care professional before rendering a decision regarding an appeal. Under the Privacy Standards, only the minimum necessary PHI to allow the medical reviewer to properly assist the fiduciary and provide a medical judgment may be disclosed. However, make sure that the medical reviewer is given enough PHI to assist the fiduciary and support his/her judgment. Further, it is recommended that either a Business Associate Agreement or Subcontractor/Agent Agreement be entered into with the medical reviewer, as appropriate, based upon the type of relationship with the plan.

Additionally, ERISA requires that a plan maintain documentation to substantiate certain filings that are required (e.g. Form 5500s) by the Department of Labor for not less than six years after the filing date. However, the Privacy Standards require that documentation (policies and procedures) be kept for six years from the date of its creation or the date when last in effect, whichever is later. Thus, plans may need to amend their record retention policies to comply with the Privacy Standards, which may require longer retention in some cases.

2. What are the "reasonable safeguards" we must take?

HHS has made it clear that it does not expect a Covered Entity to make structural changes, such as soundproofing walls, providing private rooms or other changes to make sure that conversations are not overheard or that computer screens are not seen by unauthorized individuals. Rather, HHS contemplates changes such as adding curtains or screens or cubicles to areas where oral communications between plan participants and the Plan Administrator take place, placing a fax machine that receives PHI in an area where access is limited to those who are authorized to use PHI, locking files that contain PHI in written form, placing computers in areas where only those who are authorized to access PHI can see the screens and putting passwords in place on computers containing PHI.

3. What are the penalties for non-compliance?

Covered Entities that violate the Privacy Standards can face the following:

- Civil penalties from \$100 per incident, up to \$25,000 per person, per year, per standard; and
- Criminal penalties up to:

- \$50,000 and one year in prison for obtaining or disclosing PHI in violation of the Privacy Standards;
- \$100,000 and up to five years in prison for obtaining PHI under false pretenses; and
- \$250,000 and up to 10 years in prison for obtaining or disclosing PHI with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

Keep in mind that corporations and other entities cannot serve prison time; therefore, personal liability attaches to those who violate the Privacy Standards.