d. Responsibilities of the Privacy Official

The Privacy Official will monitor the PHI that a Business Associate must return to the Plan or destroy (or extend the protections of the Business Associate Agreement if the PHI is not returned or destroyed) upon termination of the Business Associate Agreement.

The Privacy Official will ensure that all complaints about privacy violations by a Business Associate are reviewed according to the Plan's procedures, as described in Section 6.03.

If the Privacy Official knows of acts or a pattern of activity by a Business Associate that are a material violation of the Business Associate Agreement, the Privacy Official will take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the Privacy Official will determine, in consultation with the Plan's Administrator whether termination of the Business Associate Agreement is feasible. If not feasible (i.e., there are no viable business alternatives for the Plan), the Privacy Official will report the violation to HHS.

e. Documenting Business Associate Agreements

All Business Associate Agreements will be retained for a period of six (6) years from the date they were last in effect.

f. Citations

45 CFR § 164.502(e)(1)
45 CFR § 164.504(e)

7.06 Authorization

The HIPAA Privacy Rule requires the Plan to receive an Authorization from a Participant before using or disclosing PHI for purposes other than Treatment, Payment, Health Care Operations, or as otherwise permitted or required by the HIPAA Privacy Rule. The Plan may act on an Authorization only to the extent consistent with the terms of such Authorization.

a. Providing the Authorization Form to Participants

The Plan's Administrator will provide an Authorization Form (see Section 10.08(f)) to Participant who requests that his or her PHI be disclosed to a third party (other than a personal representative).

The Plan's Administrator will provide each Participant with an Authorization Form if the Plan's Administrator wants to use or disclose the Plan's PHI for a purpose that requires Authorization (see Section 4.04).

b. Signing of the Authorization Form

The signing of an Authorization Form is voluntary. Participants may refuse to authorize use of their PHI.

c. Receiving the Signed Authorization Form

The Plan must have a signed Authorization Form from the Participant, before it can take an action that requires Authorization.

d. Determining the Validity of Authorization

Before the use or disclosure of PHI, the Plan will confirm that the Authorization is valid by verifying that:

- The expiration date or event triggering expiration has not passed;
- The Authorization was filled out completely;
- The Authorization has not been revoked; and
- The Authorization Form contains all the required elements.

e. Revocation of Authorization

At any time, the Participant may revoke the Authorization, provided that a revocation will not be effective if the Authorization was relied on as described in the Form. Requests for revocation of Authorizations must be submitted in writing to Authorization Contact (see Section 10.03). The Plan will not act upon an Authorization that has been revoked.

f. Documentation Requirement

All Authorizations and revocations of Authorizations will be documented and retained for a period of six (6) years from the date the Authorization is created or when it last was in effect, whichever is later.

g. Citations

45 CFR § 164.508

8. Definitions

8.01 Definitions

Authorization: A person's permission to use PHI for purposes *other* than Treatment, Payment, or Health Care Operations, or as otherwise permitted or required by the HIPAA Privacy Rule (see Section 4). Authorizations require specific contents described in Section 7.06.

Business Associate: A person or entity that performs a function or activity regulated by HIPAA on behalf of the Plan and involving individually identifiable health information. Examples of such functions or activities are claims processing, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial services. A Business Associate may be a Covered Entity. However, Insurers and HMOs are not Business Associates of the plans they insure. The HIPAA Privacy Rule requires that each Business Associate of the Plan enter into a written contract (Business Associate Agreement) with the Plan before the Plan can disclose PHI to it, as described in Section 7.05.

Covered Entity: A health plan (including an employer plan, Insurer, HMO, and government coverage such as Medicare); a health care provider (such as a doctor, hospital, or pharmacy) that electronically transmits any health information in connection with a transaction for which HHS has established an EDI (electronic data interchange) standard; and a health care clearinghouse (an entity that translates electronic information between nonstandard and HIPAA standard transactions).

De-identification: The removal of personal information (such as name, Social Security number, address) that could identify an individual. The HIPAA Privacy Rule lists eighteen (18) identifiers that must generally be stripped for data to meet the De-identification safe harbor described in Section 4.06.

Designated Record Set: A group of records that the Plan (or its Business Associate) maintains that relates to enrollment, Payment, claims adjudication, and case or medical management records, or that the Plan (or its Business Associate) uses, in whole or in part, to make decisions about Participants. The Plan has identified specific Designated Record Sets for particular uses (see Section 5.02).

Disclosure: The release, transfer, provision of access to, or divulging in any other manner of PHI outside of the Plan.

ERISA: The Employee Retirement Income Security Act of 1974, as amended.

Fiduciary: A person or entity that exercises any discretionary authority or discretionary control respecting management of the Plan or disposition of its assets; renders investment advice for a fee or other compensation, direct or indirect, with respect to any moneys or other property of the Plan, or has authority or responsibility to do so; or has discretionary authority or discretionary responsibility in the administration of the Plan. A Fiduciary can be an individual, partnership,

joint venture, corporation, mutual company, joint-stock company, trust, estate, association, unincorporated organization, or employee organization. A person can be deemed a Fiduciary by performing the acts described above with or without authority to do so, by holding certain positions with duties and responsibilities similar to the acts described above, or by being expressly designated or named as a Fiduciary in the Plan Document.

Health Care Operations: Activities related to a Covered Entity's functions as a health plan, health provider, or health care clearinghouse. They include quality assessment and improvement activities, credentialing, training, accreditation activities, underwriting, premium rating, arranging for medical review and audit activities, business planning and development (such as cost management), customer service, grievance and appeals resolution, vendor evaluations, legal services.

HHS: The United States Department of Health and Human Services.

HIPAA Privacy Rule: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes "administrative simplification" rules that will affect the way group health plans and their vendors use, disclose, transmit, and secure health information. The administrative simplification rules include: privacy protections; rules governing transmission of electronic health care data (electronic data interchange or "EDI" rules); and rules that apply new security standards to health information. The "HIPAA Privacy Rule" refers to the new privacy protections of HIPAA.

Insurer: An underwriter, insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a state and is subject to state law that regulates insurance. This term does not include a group health plan.

Marketing: A communication about a product or service that encourages recipients of the communication to purchase or use the product or service, except for communication made:

- To describe a health-related product or service (or payment for such product or service) that is provided by, or included in the benefits of, the Plan, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, the Plan; and health-related products or services available only to a Plan enrollee that add value to, but are not part of, the Plan's benefits;

- For Treatment; or

- For case management or care coordination for the person, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the person.

In addition, marketing includes an arrangement between a Covered Entity and any other entity whereby the Covered Entity discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product

or service that encourages recipients of the communication to purchase or use that product or service.

Minimum Necessary: To the extent practical, individually identifiable health information should be disclosed only to the extent needed to support the purpose of disclosure. Covered Entities are expected to make a reasonable effort to limit use, disclosure of, and requests for PHI to the *Minimum Necessary*. HIPAA requires Covered Entities to make their own assessment of what health information is reasonably necessary.

Participant: Persons who are or were eligible for benefits under the Plan. Participant refers to both active employees who are members of the Plan and other beneficiaries, unless the context clearly indicates otherwise.

Payment: Activities by a plan to obtain premiums or determine or fulfill its responsibility for coverage and the provision of benefits under the Plan. Also, activities by a plan or provider to obtain or provide reimbursement for the provision of health care. These activities include determinations of eligibility or coverage, adjudication or subrogation or health benefit claims, billing, claims management, collection activities, reinsurance payment, review of health care services with respect to medical necessity, review of coverage under a health plan, review appropriateness of care or justification of charges, and utilization review activities.

Plan: The health plan for which these Policies and Procedures were written.

Plan Sponsor: The employer, employee organization, or the association, committee, joint board of trustees, or other similar group of representatives, that established or maintain the Plan.

Policies and Procedures: Descriptions of the Plan's intentions and process for complying with the HIPAA Privacy Rule, as codified in this Manual.

Privacy Official: A designated individual responsible for the development and implementation of the Plan's privacy Policies and Procedures.

Privacy Notice: A description, provided to Participants at specific times, and to other persons upon a request of the Plan's practices concerning its uses and disclosures of PHI, which also informs Participants of their rights and of the Plan's legal duties, with respect to PHI.

Protected Health Information (PHI): Individually identifiable health information created or received by a Covered Entity. Information is "individually identifiable" if it names the individual person or there is a reasonable basis to believe components of the information could be used to identify the individual. "Health information" means information, whether oral or recorded in any form or medium, that (i) is created by a health care provider, plan, employer, life Insurer, public health authority, health care clearinghouse, or school or university; and (ii) relates to the past, present, or future physical or mental health or condition of a person, the provision of health care to a person; or the past, present, or future Payment for health care.

Psychotherapy Notes: Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. It excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Treatment: The provision, coordination, or management of health care by one (1) or more health care providers. It includes health care coordination or management between a provider and a third party, as well as consultation and referrals between providers.

9. HIPAA Privacy Rule

Standards for Privacy of Individually Identifiable Health Information
Regulation Text, as amended
Table of Contents