Vanderbilt University

HIPAA Privacy Manual

As prepared by

The HIPAA Privacy Manual was drafted for the exclusive use of Vanderbilt University (Vanderbilt) to assist VANDERBILT in complying with the federal Standards for Privacy of Individually Identifiable Health Information under Title II of the Health Insurance Portability and Accountability Act of 1996, as amended (known as HIPAA). Any reproduction or other use for commercial or other purposes is not permitted without the express written permission of Mercer. Because Mercer is a consulting firm and does not practice law, we strongly recommend that the HIPAA Privacy Manual and its intended usage be reviewed by VANDERBILT's legal counsel. The contents of the HIPAA Privacy Manual have been prepared based upon sources, materials and information believed to be reliable and accurate. Mercer makes no representation or warranties as to the accuracy of the information set forth in the HIPAA Privacy Manual and accepts no responsibility or liability for any error, omission, or inaccuracy in such information other than in relation to information which Mercer would be expected to have verified based on generally accepted industry practices. Mercer does not assume responsibility for any updates to the HIPAA Privacy Manual that might become necessary as a result of VANDERBILT's subsequent plan or administrative changes or as a result of any relevant regulatory developments or changes in applicable law.

Copyright © 2015

Table of Contents

Copyright © 2015

 Copyright © 2015

 Copyright © 2015

1. Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the US Department of Health and Human Services (HHS) to establish rules to protect the privacy of health information. HHS issued detailed rules (referred to throughout this Manual as the HIPAA Privacy Rule), for health plans, health care providers, and certain other health care entities (known as Covered Entities). Health information covered by the HIPAA Privacy Rule is known as Protected Health Information (PHI).

Words and phrases that are capitalized in this Manual, such as "Covered Entities," have special meanings that are defined in Section 8.

VANDERBILT sponsors the group health plan(s) listed in Section 10.01 and each plan is a Covered Entity. Health plans and other Covered Entities are required to create Policies and Procedures to ensure their compliance with the HIPAA Privacy Rule. This Manual is designed to be the Policies and Procedures for the health plan(s) in Section 10.01, referred to throughout as the "Plan". In the event of multiple covered plans, because each plan is sponsored by VANDERBILT , they collectively comprise an "organized health care arrangement" and the Manual represents the Policies and Procedures for each plan.

The Manual consists of eleven (11) sections.

Section 1 this introduction describes the purpose of the Manual and its organization.

Section 2 describes the Plan's overall policy for protecting the use and disclosure of health information.

Sections 3 and 4 describe the basic requirements that apply to the Plan's use and disclosure of PHI. The sections also describe the procedures VANDERBILT will use when handling health information for the Plan.

Section 5 describes certain rights that Plan Participants and their beneficiaries have concerning their own PHI, and the Plan's procedures for administering those rights.

Sections 6 and 7 describe risk management requirements that the Plan must meet and documentation that the Plan must maintain. The sections also describe VANDERBILT's risk management activities for actions it performs on the Plan's behalf.

Section 8 defines key terms that are used in this Manual. The defined terms are capitalized throughout the Manual. *In general, the term Participant is used to refer to persons who are or were eligible for benefits under the Plan. Participant is used to refer to both employee Participants and other beneficiaries, unless the context clearly indicates otherwise.*

 Copyright © 2015

Section 9 contains links to the text of regulations related to implementation of this Manual.

Section 10 contains key resources related to the implementation of this Manual. It includes the name of the Privacy Official responsible for the development, coordination, implementation, and management of the Manual. It also includes key contacts (persons or offices) responsible for responding to Participants exercising their rights described in Section 5, for receiving complaints about the Plan's compliance with the Manual or with the HIPAA Privacy Rule, and for processing any specific Authorizations that Participants may be asked to provide concerning the use of their PHI. Finally, it includes the forms and other Plan Documents that VANDERBILT will be using to meet the privacy requirements, along with instructions for using those forms.

The Manual will be provided to employees of VANDERBILT who have access to PHI. The employees will also receive updates that reflect any changes in law or the Manual's procedures. Employees can obtain more information from the Plan's Privacy Official and other contacts listed in Section 10.

*Health information collected by VANDERBILT pursuant to other laws such as the Family and Medical Leave Act, Americans with Disabilities Act, Occupational Safety and Health Act, or workers' compensation laws, is **not** protected under HIPAA as PHI (although this type of information may be protected under other federal or state laws).*

 Copyright © 2015

2. Statement of Privacy Policy

The Plan will protect the privacy of Participants' and family members' health information (known as Protected Health Information or PHI) in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). PHI generally will be used only for health plan Payment activities and Health Care Operations, and in other limited circumstances such as where required for law enforcement and public health activities. In addition, the Minimum Necessary information will be used except in limited situations specified by law. Other uses and disclosures of PHI will not occur unless the Participant authorizes them. Participants will have the opportunity to inspect, copy, and amend their PHI as required by HIPAA. Participants can exercise the rights granted to them under HIPAA free from any intimidating or retaliatory acts.

When PHI is shared with persons and entities providing services to the Plan (Business Associates), they will be required to agree in writing to maintain procedures that protect the PHI from improper uses and disclosures in conformance with HIPAA.

When VANDERBILT receives PHI to assist in Plan administration, it will adhere to its own stringent procedures to protect the information. Among the Procedures in place are:

- Administrative and technical firewalls that limit which groups of employees are entitled to access PHI and the purposes for which they can use it;
- Rules for safeguarding PHI from improper disclosures;
- Processes to limit the disclosure of PHI to the Minimum Necessary;
- A verification process to identify and confirm the authority of persons requesting PHI;
- A training process for relevant staff; and
- Processes for filing privacy complaints.

The Plan may update this Policy and its Procedures at any time. The Plan will also update this Policy and its Procedures to reflect any change required by law. Any changes to this Policy and Procedures will be effective for all PHI that the Plan may maintain. This includes PHI that was previously created or received, not just PHI created or received after the Policy and Procedures are changed.

Copyright © 2015

3. Safeguards

 Copyright © 2015

3.01 Overview

The Plan will develop and implement administrative, technical, and physical safeguards that will reasonably protect Protected Health Information (PHI) from intentional and unintentional uses or disclosures that violate the HIPAA Privacy Rule. In addition, the Plan will institute procedures to verify the identity of any person or entity requesting PHI and the authority of that person or entity to have access to PHI.

PHI is individually identifiable health information created or received by a Covered Entity. Information is "individually identifiable" if it identifies the individual 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 or received by a health care provider, health 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.

Sections 3.02 and 3.03 describe the Procedures VANDERBILT will use to establish safeguards and to verify identification and authority when using PHI. Insurers and Business Associates of the Plan should also adopt procedures that meet the requirements of the HIPAA Privacy Rule.

 Copyright © 2015

3.02 Protection Procedures

VANDERBILT or the VANDERBILT's vendors will apply the following Procedures to protect PHI:

Protected information	Protection procedures
Printed/ hard copy documentation	• Funnel incoming mail through distinct channels to limit the number of people with access to PHI. • Limit the number of photocopies made of PHI. • Implement a "clean desk" practice. PHI will be put away if the employee is away from his or her desk throughout the day and PHI will be placed in closed and locked HR/Benefits cabinets for storage. • PHI that the Plan is required to retain for lengthy time frames may be kept in off-site storage areas, with access limited to designated personnel. PHI in paper format will be destroyed when it is obsolete or is not required to be retained for storage purposes, with shredding the preferred method of destruction.
E-mail and electronic storage (LAN/hard drive/diskettes)	• Destroy electronic PHI that is no longer needed, including cutting or destroying CDs or diskettes so that the data is not readable or capable of reconstruction. • Limit the use of PHI in e-mails, to the extent practical, to the Minimum Necessary to accomplish the intended purpose (e.g., refrain from forwarding strings of e-mail messages containing PHI. Instead, prepare a new message with PHI essential to the task). • Encrypt e-mail set outside organization that includes PHI. • Require password entry each time an employee accesses the e-mail system. • Use "locking" screensavers to limit access. • Maintain and periodically update network monitoring software, including intrusion detection and reporting. • Maintain and periodically update systems for backing up data and contingency plans for data recovery in the event of a disaster. • Maintain and periodically update systems for tracking access and changes to data.

 Copyright © 2015

Protected information	Protection procedures
	• Periodically review the process for handling system maintenance and the hardware/software acquisition process. • Maintain and periodically update virus software and protection processes. • Maintain and periodically review procedures for ending data access for staff (e.g., after they terminate employment). • Follow other company IT guidelines regarding electronic data. • Limit remote access to systems to secure methods
Facsimiles	• Ensure that fax machines used foe plan administration are not located in publicly accessible areas • Develop fax coversheet including confidentiality statement and warning about releasing data. • Limit faxing of PHI to urgent information. • Notify the receiver in advance that VANDERBILT is sending a fax with PHI so he or she can retrieve it immediately. • Check confirmation sheets to verify that outgoing faxes with PHI were received by the correct number.
Oral conversations/ telephone calls/voicemail	• Limit the content of PHI in conversations (e.g., with vendors and other staff), as practical, to the Minimum Necessary to accomplish the intended purpose. • Verify the identity of individuals on the phone (see Section 3.03). • Implement reasonable measures to prevent other individuals from overhearing conversations inclusive of PHI, including conducting oral conversations re PHI in closed offices when possible or not using speaker phone when conversation could be overheard • Limit voicemail messages, or messages left for other individuals, to high-level information to ensure no one else could over hear PHI.

Copyright © 2015

3.03 Verification Procedures

In performing administration activities for the Plan, VANDERBILT will implement the following verification procedures to reasonably ensure the accurate identification and authority of any person or entity requesting PHI. Note that documentation of these verifications should be retained as provided in Section 6.06. Insurers and Business Associates should also institute verification procedures for disclosures of PHI.

Who makes the request	Procedure
Participants, Beneficiaries, and others acting on their behalf	VANDERBILT may obtain photo identification, a letter or oral authorization, marriage certificate, birth certificate, enrollment information, identifying number, and/or claim number.
Health plans, providers, and other Covered Entities	VANDERBILT may obtain identifying information about the entity and the purpose of the request, including the identity of a person, place of business, address, phone number, and/or fax number known to the Plan.
Public officials	For in-person requests, obtain agency identification, official credentials or identification, or other proof of government status. For written requests, verify they are on the appropriate government letterhead. Also obtain a written (or, if impracticable, oral) statement of the legal authority under which the information is requested.*
Person acting on behalf of a public official	Obtain a written statement on appropriate government letterhead or other evidence or documentation of agency (such as a contract for services, memorandum of understanding, or purchase order) that establishes that the person is acting on behalf of the public official.
Person acting through legal process	Obtain a copy of the applicable warrant, subpoena, order, or other legal process issued by a grand jury or judicial or administrative tribunal.
Person needing information based on health or safety threats	Consult with Privacy Official. Disclosure is permitted if, in the exercise of professional judgment, VANDERBILT concludes the disclosure is necessary to avert or lessen an imminent threat to health or safety, and that the person to whom the PHI is disclosed can avert or lessen that threat.

*VANDERBILT will rely on the statements and documents of public officials unless such reliance is unreasonable in the context of the particular situation.

Copyright © 2015

a. Citations

45 CFR § 164.514(h)

 Copyright © 2015

4. Uses and Disclosures

 Copyright © 2015

4.01 Overview

This Section 4.01 summarizes limits imposed by the HIPAA Privacy Rule on the Plan's uses and disclosures of PHI. Sections 4.02 through 4.06 describe Procedures VANDERBILT maintains to satisfy the standards when it uses PHI on behalf of the Plan. Section 4.07 provides a Procedure for alerting the Breach Contact to impermissible uses and disclosures. Insurers and Business Associates should also adopt procedures to meet the HIPAA standards, and Business Associates will act as described in their Business Associate Agreement (see Section 7.05).

In general, a Participant's PHI can be used or disclosed for a variety of Plan administrative activities. Common examples include paying claims, resolving appeals, managing specialty vendors and helping Participants address problems. The HIPAA Privacy Rule does not prohibit these activities, but it imposes the following guidelines:

Uses and disclosures generally allowed without Authorization. A person's PHI can be used or disclosed by the Plan without obtaining that person's Authorization as follows:

- If disclosed to VANDERBILT for enrollment activities and (where only summary health information is used) for premium bids (except that genetic information may not be used for this purpose) and Plan Amendment/termination activities;
- If requested by a Health Care Provider for Treatment;
- If needed by the Plan for Payment activities such as claims, appeals, and bill collection;
- If needed by the Plan for Health Care Operations such as audits and wellness and risk assessment programs;
- If disclosed to the Participant, and in certain circumstances, to family members and others acting on the Participant's behalf; and
- If required by law, in connection with public health activities, or in similar situations as listed in Section 10.10.

Details on the types of activities that constitute permissible uses or disclosures for Treatment, Payment, or Health Care Operations purposes are included in Section 8. In some cases, the Plan will want to use or disclose PHI for other purposes, in which case Authorization will be required. In addition, except in certain limited circumstances, Authorization is required for the use and disclosure of Psychotherapy Notes and for the use or disclosure of PHI for Marketing purposes.

Limiting PHI use or disclosure to the "Minimum Necessary." To the extent practical, the Plan must limit uses and disclosures of, and requests for, PHI to the Minimum Necessary

 Copyright © 2015

amount of PHI needed to accomplish the intended purpose of each transaction. The workforce member will exercise judgment as to the amount of PHI needed and that amount will be considered the Minimum Necessary in that case. This requirement does not apply to:

- Uses or disclosures for Treatment purposes;
- Disclosures to the Department of Health and Human Services (HHS) for audits of the Plan's compliance with the HIPAA Privacy Rule;
- Disclosures to an individual of his or her own PHI;
- Uses or disclosures required by law;
- Uses or disclosures made pursuant to an Authorization; and
- Uses or disclosures otherwise required for compliance with the HIPAA Privacy Rule.

Deidentified Information. The limits in this Manual apply only to health information that is individually identifiable. If information is deidentified to the extent required by the Privacy Rule, it can then be used or disclosed without restriction. Workforce members can consult the Privacy Official as to what constitutes sufficient deidentification. In addition, information that has most of its identifiers removed can be disclosed to a person signing a Data Use Agreement (see Section 4.06).

Improper Uses or Disclosures. The Plan's PHI cannot be properly used or disclosed except as described in this Manual. If VANDERBILT workforce members learn of a suspected or confirmed improper use or disclosure of PHI, they are required to take timely action so that VANDERBILT may meet its obligations to assess and address the incident (see Section 4.07).

a. Citations

45 CFR § 164.502(b)
45 CFR § 164.502(d)
45 CFR § 164.508
45 CFR § 164.514
45 CFR part 164, subpart D

 Copyright © 2015

4.02 Enrollment, Premium Bids, and Amendment/Termination Activities

VANDERBILT will process Participant enrollment and disenrollment elections and transmit the elections to the Plan, its Insurers, and its Business Associates. The Plan, its Insurers and its Business Associates will, without obtaining a Participant's Authorization, disclose certain types of PHI (enrollment/disenrollment information and summary health information) to VANDERBILT (or its agents) in the following circumstances:

PHI disclosed	Employer uses of PHI
Enrollment and disenrollment information	• Enrollment and disenrollment activities, including processing of annual enrollment elections, payroll processing of elected Participant contribution amounts, new-hire elections, enrollment changes, and responding to Participant questions related to eligibility for Plan enrollment.
Summary health information (see table below)	• To obtain premium bids for health insurance coverage under the Plan (if VANDERBILT requests the information). Genetic information may not be used for this purpose. • To modify, amend, or terminate the Plan (if VANDERBILT requests the information).

The enrollment and disenrollment information and summary health information that VANDERBILT receives from the Plan will not be subject to the provisions of this Manual.

 Copyright © 2015

Required deletions for Summary Health Information		
Summary health information is information that summarizes claims history, expenses, or types of claims of individuals receiving benefits under the Plan from which the following information has been deleted.		
• Names • Social Security numbers • Full face photographic and any comparable images • Telephone numbers • Specific dates such as dates of birth and death, and admission/discharge dates. *The Plan can use the year of the event, except for the birth year of persons over age eighty-nine (89)*	• Vehicle identifiers (serial number or license plate number) • Device identifiers and serial numbers • Web Universal Resource Locators (URLs) • Fax numbers • E-mail address • Medical record number • Any other unique identifying numbers, or characteristics, or codes, including particular subsidiaries, divisions, or work locations	• Health plan beneficiary numbers • Account numbers • Certificate/license numbers • Internet Protocol (IP) address numbers • Biometric identifiers (e.g., finger, iris, or voice prints) • Geographic identifiers smaller than a state, including street address, city, county, and precinct; but the five (5)-digit zip code may be used.

a. Citations

45 CFR § 164.504(f)(1)

Copyright © 2015

4.03 Treatment, Payment, and Health Care Operations

The HIPAA Privacy Rule permits VANDERBILT to receive PHI from the Plan without Authorization only after VANDERBILT has amended the Plan and certified that it will limit uses and disclosures of PHI to Plan administrative activities and will otherwise protect PHI as required by the law. The Plan's certification and amendment are in Sections 7.03 and 7.04. This Section 4.03 describes VANDERBILT's procedures for using or disclosing PHI for Plan administrative activities without Authorization. In general, VANDERBILT will:

- Identify the classes of employees with access to PHI and the categories of information they will use;
- To the extent practical, make reasonable efforts to limit disclosures of and requests for PHI to a Limited Data Set or, if needed, the Minimum Necessary to accomplish the intended purpose;
- Maintain procedures governing the storage of PHI; and
- If feasible, return or destroy PHI received from the Plan, and maintain procedures governing the retention and destruction of PHI not returned or destroyed.

Procedures governing disclosures and requests made on a routine and recurring basis are described in the following charts. For other disclosures and requests, VANDERBILT will review each situation on an individual basis by considering the importance of the request or disclosure; the costs of limiting the request or disclosure; and any other factors VANDERBILT believes to be relevant. Any uses or disclosures of PHI not included in these tables but permitted to be made without Authorization in the Notice of Privacy Practices (see Section 7.02) should be made after consultation with the Privacy Official if feasible.

 Copyright © 2015

a. Appeals of Adverse Benefit Determinations

VANDERBILT **staff may process final appeals to adverse benefit determinations for the self funded plans. Process includes collecting information relevant to benefit determinations; review and analysis; documenting decisions; corresponding with Participants to apprise them of status and final determination; communicating with Business Associates as appropriate. This is a Payment activity.**	
VANDERBILT staff permitted access to PHI	• Those employees listed in Access Control list in Plan's Security Manual involved in Appeals of Adverse Benefit Determinations.
Parties to whom disclosures are permitted	• Participant who is the subject of the appeal, and associated individuals as permitted by Section 4.05. • Health care providers involved with treating the Participant • Business Associates involved in the initial benefit determination. • Business Associates (including health care professionals) assisting with review and analysis of the benefit determination and appeal.
Categories of PHI	• Information relating to appeals, including: – copies of the denial letter and appeal decision letter. – documents submitted by the claimant, health care providers, etc. – benefit determinations of Participants receiving similar services.
Protocols for meeting Minimum Necessary requirement	• PHI will be Deidentified (e.g., name and location removed) to the extent possible by Business Associates or by HR employees before the claim is forwarded for review. Further, if complete Deidentification isn't possible, the Business Associate or HR employees will use reasonable efforts to determine the minimum amount of PHI that is directly relevant to the performance of the task.
Storage of PHI	• Paper records will be maintained in the HR/Benefits file room or other secure location and clearly labeled "Plan Appeals." • Electronic records will be retained consistent with the Plan's HIPAA Security Manual. • Information will be protected using the procedures in Section 3.02.
Retention/ Destruction	• No redundant copies will be retained. • PHI will be destroyed when no longer needed or 6 years after creation.

 Copyright © 2015

b. Customer Service

HR staff assist Participants with various eligibility and claims questions. Process involves intake of questions from Participants, collecting information relevant to questions; documenting decisions; communicating with Participants to apprise them of status and resolution; communicating with Business Associates and Insurers as appropriate. This is a Payment activity.	
VANDERBILT staff permitted access to PHI	• Those employees listed in Access Control list in Plan's Security Manual involved in Customer Service activities.
Parties to whom disclosures are permitted	• Participant who is the subject of a question, and associated individuals as permitted by Section 4.05. • Health care providers involved with treating the Participant • Business Associates and Insurers involved in benefit determinations. • Business Associates Insurers assisting with review and analysis of benefit determinations.
Categories of PHI	• All PHI relevant to the claim.
Protocols for meeting Minimum Necessary requirement	• VANDERBILT staff will use reasonable means to determine the minimum amount of information necessary that, in their judgment, is directly relevant to the resolution of the question. • Questions about the scope of requested disclosures should be directed to the Privacy Official.
Storage of PHI	• Paper records will be maintained in the HR/Benefits file room or other secure location and clearly labeled "Customer Service." • Electronic records will be retained consistent with the Plan's HIPAA Security Manual. • Information will be protected using the procedures in Section 3.02.
Retention/ Destruction	• No redundant copies will be retained. • PHI will be destroyed when no longer needed or 6 years after creation.

 Copyright © 2015

c. Data Analysis

VANDERBILT **staff perform plan auditing, rate setting and benefits planning and analysis using claims and appeals information obtained from Business Associates and Insurers. Business Associates perform claim data collection and warehousing services and provide reports to** VANDERBILT **for the purpose of performing trending, forecasting, and cost calculations. These are both Health Care Operations activities and Payment activities.**	
VANDERBILT staff permitted access to PHI	• Those employees listed in Access Control list in Plan's Security Manual involved in Data Analysis.
Parties to whom disclosures are permitted	• Business Associates involved in data aggregation. • Business Associates assisting with review and analysis of data.
Categories of PHI	• All claims data related to Participants, but excluding any physician notes and underlying claim records.
Protocols for meeting Minimum Necessary requirement	• Business Associate will use reasonable means to determine the minimum amount of information necessary to be provided before providing PHI to VANDERBILT.
Storage of PHI	• Paper records will be maintained in the HR/Benefits file room or other secure location and clearly labeled "Data Analysis." • Electronic records will be retained consistent with the Plan's HIPAA Security Manual. • Information will be protected using the procedures in Section 3.02.
Retention/ Destruction	• No redundant copies will be retained. • PHI will be destroyed when no longer needed or 6 years after creation.

d. Citations

45 CFR § 164.506

Copyright © 2015

4.04 When Authorizations are Needed

VANDERBILT will obtain a Participant's Authorization for any use or disclosure of PHI not identified in Section 4.01, including any uses for employment-related or non-Plan-related purposes.

Authorizations will also be obtained for the use or disclosure of Psychotherapy Notes or for the use or disclosure of PHI for Marketing, except in limited circumstances identified in the HIPAA Privacy Rule, or prior to any sale of PHI. (VANDERBILT will review any request for disclosure of information that may qualify as Psychotherapy Notes or Marketing on an individual basis, in consultation with the Privacy Official, to determine whether the requirements of the HIPAA Privacy Rule are satisfied.)

PHI will not be used or disclosed on the basis of an Authorization, unless it is verified that the Authorization:

- Has not expired;
- Has not been revoked; and
- Includes all required information.

The requirements for Authorizations are described in Section 7.06.

A copy of each Authorization will be retained for six (6) years from the later of the date the Authorization was created or the last date the Authorization was effective.

a. Citations

45 CFR § 164.508

Copyright © 2015

4.05 Disclosure to Participants, Beneficiaries, and Others Acting on Their Behalf

This Section 4.05 describes VANDERBILT's procedures for disclosing PHI to Participants, their personal representatives, and family members and others acting on their behalf. Before disclosing any PHI, VANDERBILT will verify the identity of the person requesting the information (see Section 3.03).

a. Participants

A Participant's own PHI may be disclosed to the Participant without Authorization.

b. Personal Representatives

A personal representative will be treated as the Participant and the Participant's PHI may be disclosed to the personal representative without Authorization. VANDERBILT will make reasonable efforts to limit disclosures with respect to PHI to the information relevant to such personal representation. A person will be treated as a personal representative in accordance with the following table and applicable state law. However, see the discussion following this table for important restrictions on personal representative status.

Participant	Person requesting PHI	Personal representative?
Minor child	Parent or guardian*	Yes, but must provide proof of relationship.
Adult child	Parent or guardian	Yes, but must provide proof of relationship.
Adult	Spouse or other adult	Yes, but only upon proof of legal authority (e.g., court order) or voluntary agreement (e.g., power of attorney).
Deceased	Executor or Administrator In some cases family member of others involved in the care or payment for the care of the individual	Yes, but only upon proof of legal authority (e.g., provisions of a will or power of attorney). In certain cases, the Plan may determine that certain family members or others who were involved in the care of the individual, or payment for that care would be an appropriate Personal representative.

*This includes a person with the legal authority to make health care decisions.

 Copyright © 2015

Restrictions Regarding Minor Children

VANDERBILT generally will treat the parent (or guardian or other person acting in the place of a parent) of a minor child as the child's personal representative, in accordance with applicable state law. However, the parent will not be treated as the personal representative for PHI related to health care services received by the minor if:

- The minor lawfully obtained the services with the consent of someone other than the parent, who is authorized by law to give that consent (e.g., a court);
- The minor lawfully consented to and obtained the services and state law does not require the consent of anyone else; or
- The parent assents to a confidentiality agreement between the health care provider and the minor with respect to the services.

If a parent is not treated as a minor child's personal representative for a particular service, the parent may still receive access to the child's PHI under the individual right to inspect and copy PHI (Section 5.02) if the decision to provide access is made by a licensed health care professional, in the exercise of his or her professional judgment, and the decision is consistent with state law.

Restrictions Regarding Abuse or Endangerment

VANDERBILT may elect not to treat a person as a Participant's personal representative if, in the exercise of professional judgment, VANDERBILT decides that it is not in the best interest of the Participant because of a reasonable belief that:

- The Participant has been or may become subject to abuse, domestic violence, or neglect by the person; or
- Treating the person as a personal representative could endanger the Participant.

A Participant may request that the Plan limit communications with a personal representative by submitting a request for Confidential Communications (see Section 5.05).

c. Others Acting on a Participant's Behalf

The HIPAA Privacy Rule provides discretion to disclose a Participant's PHI to any individual without Authorization if necessary for Payment or Health Care Operations. This can include disclosures of a Participant's PHI to the Participant's family members. In making these disclosures, VANDERBILT will make reasonable efforts to limit disclosures to the Minimum Necessary to accomplish the intended purpose.

 Copyright © 2015

In certain additional cases, PHI can be disclosed without Authorization to a Participant's family members, friends, and others who are not personal representatives, if any of the following conditions applies:

- Information describing the Participant's location, general condition, or death is provided to a family member or other person responsible for the Participant's care (including PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts);
- PHI is disclosed to a family member, close friend or other person identified by the Participant who is involved in the Participant's care or Payment for that care, and the Participant had the opportunity to agree or object to the disclosure; or
- PHI is disclosed to a family member or friends involved in the Participant's care and it is impossible (due to incapacity, emergency or death) to obtain the Participant's agreement.

d. Citations

45 CFR § 164.502(g)
45 CFR § 164.510

Copyright © 2015

4.06 Use and Disclosure of Deidentified Information and Data Use Agreements

Health information can be used without complying with the limits in this Manual if names, Social Security numbers and other data are removed so there is no reasonable basis to believe it can be used to identify a person – it is "deidentified". A Plan may choose to deidentify PHI and then use it without written Authorization from the persons to whom it pertains. A Plan can also remove most identifying data and disclose it without Authorization for selected purposes if the recipient agrees to protect the data through a Data Use Agreement.

Insurers and Business Associates acting on behalf of the Plan should adopt procedures for applying these Deidentification rules and entering into Data Use Agreements. VANDERBILT's procedures are described in this Section.

a. Deidentified Information

To deidentify Plan information, the specific data in the following list will be removed. However, if VANDERBILT knows that, despite the removal of these data elements, the information could still be used to identify a person, it will be protected as PHI.

- Names;
- Social Security number;
- Specific dates such as dates of birth and death, and admission/discharge dates. *The Plan can use the year of the event, except for the birth years of persons over age eighty-nine (89)*
- Telephone numbers;
- Fax numbers;
- E-mail addresses;
- Medical record numbers;
- Health plan beneficiary number;
- Geographic identifiers smaller than a state, including street address, city, county, precinct, and zip code. *The first three (3) numbers of the zip code can be used if more than 20,000 people are in any combination of zip codes with the same first three (3) numbers;*
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers (serial numbers or license plate numbers);
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers (e.g., finger, iris, or voice prints);
- Full-face photographic and any comparable images; and
- Any other unique identifying numbers or characteristics or codes, including a particular subsidiaries, divisions or work locations.

 Copyright © 2015

The Plan can retain a code (or other method) for re-identifying a person's information in the future, if the identification mechanism will not be used or disclosed and cannot be translated so as to identify the person. If the health information is re-identified, the Plan will treat it as PHI subject to this Manual.

As an alternative to removing all the items above, a case-by-case decision can be made about how much data needs to be removed in order to deidentify information. To do so, a written statement and analysis must be obtained from an appropriate expert in statistics and information deidentification. The statement must conclude that the risk is very small the information could be used (alone or in combination with other information) to identify an individual.

b. Data Use Agreements

In limited circumstances, PHI may be disclosed without Authorization under a data use agreement. This type of disclosure is permitted upon receipt of a request for health information needed for research purposes or public health activities, if the request fails to meet the requirements in Section 10.10. The same procedures can be used to disclose PHI without Authorization for certain types of Health Care Operations not specifically described in Section 8.

For example, a data use agreement may be used to disclose information for research that has not been approved by a review board; for public health activities undertaken by private organizations instead of public health authorities; and for Health Care Operations by providers or other health plans that do not have a prior or current relationship with the subject of the PHI.

To disclose PHI without Authorization in these circumstances, the Plan must:

- Create a Limited Data Set by removing most of the identifying data listed in the table in Section 4.06(a). If all of the data is removed, the information is deidentified and can be used or disclosed without restriction. Key dates (birth date, admission/discharge date, date of death) and certain geographic information, such as city and zip code, may be retained; and

- Receive assurances from the recipient of the data that it will protect the information through a data use agreement. The agreement must establish the permitted uses and disclosures of the information, limit who can use or receive it, and promise that the recipient will safeguard the information and notify the Plan in the event the data is subject to a breach.

VANDERBILT will review each request for disclosure of information that may qualify for data use agreements on an individual basis, in consultation with the Privacy Official, to determine whether the requirements in the HIPAA Privacy Rule are satisfied.

 Copyright © 2015

c. Citations

45 CFR § 164.514
45 CFR § 164.502(d)

 Copyright © 2015

4.07 Reporting Improper Access, Uses and Disclosures

If PHI is accessed, used, or disclosed in any way not permitted by the provisions of this Manual, then such access, use, or disclosure is improper (called a "breach"). If a PHI breach occurs, the Plan must investigate facts about the incident, assess whether and who must be notified of the event, and evaluate alternative ways to prevent a similar occurrence in the future (see Section 6.05). Federal law protects staff from any type of retaliation for reporting any incident if the staff member has a good faith belief that a HIPAA violation has occurred.

VANDERBILT staff must report to the Plan's Breach Contact designated in Section 10.03 all PHI breaches as soon as they are discovered. VANDERBILT staff will report both confirmed breaches and suspected incidents for which there is a reasonable belief that a breach has occurred or is occurring.

a. How to Report a PHI Breach

An VANDERBILT workforce member will complete a Breach Incident Report Form (Section 10.09(a)) and e-mail it or send it by facsimile to the Plan's Breach Contact listed on the Form 10.09(a).

In the case of an ongoing incident or series of incidents, rather than a completed event that occurred in the past, the VANDERBILT workforce member will immediately contact the Breach Contact and communicate the information required on the Form 10.09(a).

b. What Information to Include in a Breach Report

Workforce members must complete all sections of the Form 10.09(a) as fully as possible.

If the workforce member is uncertain of the exact number of individuals whose PHI was used or disclosed in the incident, a reasonable estimate should be provided.

c. When to Submit a Breach Report

In the case of confirmed or suspected PHI breach incidents that are not ongoing, workforce members are to complete the Form 10.09(a) within two business days of discovering the incident.

If the breach is, or is suspected of being, a continuing type of event rather than one which has occurred wholly in the past, VANDERBILT workforce members should contact the Breach Contact as soon as the member reasonably believes that a continuing incident is occurring.

 Copyright © 2015

d. Documentation

VANDERBILT will maintain all Breach Incident Report Forms submitted to the Breach Contact for a period of six (6) years.

e. Citations

45 CFR Part 164, Subpart D

 Copyright © 2015

5. Individual Rights

 Copyright © 2015

5.01 Overview

The HIPAA Privacy Rule provides individuals with certain rights associated with their PHI that the Plan (and all other Covered Entities) must follow. These include the rights to:

- Access, inspect, and copy certain PHI within a Designated Record Set (see Section 5.02);
- Request the Amendment of their PHI in a Designated Record Set (see Section 5.03);
- Request restriction of the use and disclosure of their PHI (see Section 5.04);
- Request the use of alternative means or alternative locations for receiving communications of their PHI (see Section 5.05); and
- Request an accounting of PHI disclosures (see Section 5.06).

Section 10.03 identifies the contact persons for processing Participants' requests to exercise these rights.

 Copyright © 2015

5.02 Inspect and Copy PHI

a. Participant's Rights

A Participant has the right to access, inspect, and copy his or her PHI within a Designated Record Set for as long as the PHI is maintained in the Designated Record Set. A Participant may also request that such PHI be sent to another entity or person, so long as that request is clear, conspicuous, specific and signed by the Participant. The Plan must generally honor these rights, except in certain circumstances the Plan may deny the right to access. The Plan may provide a summary or explanation of the PHI instead of access or copies, if the Participant agrees in advance and pays any applicable fees.

Copies of Electronic Health Records. A Participant may request an electronic copy of his PHI (or summary or explanation) in the form or format of his choosing if his PHI is readily producible in such form or format or in such form or format that the Plan and the Participant agree on. A Participant may also request that such PHI be sent to another entity or person, so long as that request is clear, conspicuous, specific and signed by the Participant. The Plan may charge the Participant a reasonable fee for these copies that is no greater than the Plan's labor costs.

A Designated Record Set is a group of records that the Plan maintains for enrollment, Payment, claims adjudication, case management, or medical management or that the Plan uses, in whole or in part, to make decisions about Participants. Although a Designated Record Set includes the Plan's enrollment and Payment information, it does not include VANDERBILT's enrollment and payment records. The Plan will require Business Associates to identify those portions of the Designated Record Set that they maintain and to make them available for inspection and copying. VANDERBILT may maintain the following Designated Record Sets, which are available to be inspected or copied:

- Appeals of Adverse Benefit Determination documentation.

b. Processing a Request

The Plan is responsible for receiving and processing requests for access, inspection, and copying of PHI maintained in Designated Record Sets. The Plan has assigned this responsibility to Inspection Contact (see Section 10.03). If the Plan does not maintain the PHI identified in the Participant's request but knows where it is maintained, Inspection Contact will inform the Participant where to direct the request. The Plan will develop procedures to coordinate inspection of Designated Record Sets in Business Associates' custody.

Requests for access, inspection, and copying of PHI must be submitted on the Request for Access Form (Form 10.08(a)) and sent to Inspection Contact.

 Copyright © 2015

Inspection Contact will determine whether to approve or deny the request to access, inspect, or copy the PHI, in consultation with the Privacy Official, as needed.

Inspection Contact will respond to a Participant's request within thirty (30) days of the receipt of the request. If Inspection Contact is unable to respond within this timeframe, he or she will send the Participant written notice that the time period for reviewing the request will be extended for no longer than thirty (30) more days, along with the reasons for the delay and the date by which Inspection Contact expects to address the request.

c. Accepting a Request to Access, Inspect, or Copy

If Inspection Contact accepts the request, a copy of Form 10.08(a) indicating that the request has been accepted will be sent to the Participant and access will be provided within the thirty (30) day timeframe. A fee may be charged to the Participant for copying and mailing, based on the actual cost. Form 10.08(a) will inform the Participant of the fees in advance, and give the Participant an opportunity to withdraw the request if he or she does not agree to the fees.

d. Denying a Request to Access, Inspect, or Copy (Where Participant has Right to Review)

If Inspection Contact denies the request, a copy of Form 10.08(a) indicating that the request has been denied will be sent to the Participant within the thirty (30) day timeframe. Form 10.08(a) will indicate whether the Participant has the right to a review of the denial.

The Participant has the right to have the denial reviewed if Inspection Contact denies access to PHI for any of the following reasons:

- A licensed health care professional determines that the access is reasonably likely to endanger the life or physical safety of the Participant or another person;
- The PHI contains information about another person and a licensed health care professional determines that the access is reasonably likely to cause substantial harm to the other person; or
- The request is made by a personal representative, and a licensed health care professional determines that providing access to the personal representative is reasonably likely to cause substantial harm to the Participant or another person.

If Inspection Contact denies access on the basis of the risk of harm identified by a licensed health care professional, the Participant has the right to have the denial reviewed by a different licensed health care professional. Inspection Contact will promptly refer a request for review to a licensed health care professional who did not participate in the original denial decision. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access. Inspection Contact will provide or deny access in accordance with the determination of the reviewing official.

 Copyright © 2015

If Inspection Contact denies access to any PHI, the Plan will, to the extent possible, continue to provide access to other PHI for which there are no grounds to deny access.

e. Denying a Request to Access, Inspect, or Copy (Where Participant has NO Right to Review)

If Inspection Contact denies the request, a copy of Form 10.08(a) indicating that the request has been denied will be sent to the Participant within the thirty (30) day timeframe. The copy will indicate whether the Participant has the right to a review of the denial.

The Participant has no right to have a denial reviewed if Inspection Contact denies a request to access, inspect, or copy PHI, for any of the following reasons:

- The PHI is Psychotherapy Notes.
- The PHI was compiled in reasonable anticipation of, or for use in, civil, criminal, or administrative proceedings.
- The Plan maintains that the PHI is also subject to the Privacy Act (5 U.S.C. § 552a), and the Privacy Act allows the denial of access.
- The Plan received the PHI from someone (other than a health care provider) a promise of confidentiality, and allowing access to the PHI would be reasonably likely to reveal the source.
- The Plan has temporarily suspended access to PHI created for research involving Treatment, if the Participant agreed to the suspension of access when agreeing to participate in the research.

f. Form for Denial

If the request for access is denied, Inspection Contact will within the timeframes, provide a written denial (see Section 10.08(a)) to the Participant in plain language which contains:

- The basis for the denial;
- A statement of the individual's review rights, if any; and
- A description of how the individual may complain to the Plan using the complaint procedure in Section 6.03 or to HHS.

g. Documenting Requests

All requests, acceptances, and denials of PHI will be documented and retained for a period of

 Copyright © 2015

six (6) years.

h. Citations

45 CFR § 164.524

 Copyright © 2015

5.03 Amend PHI

a. Participant's Rights

A Participant has the right to request that the Plan amend his or her PHI in a Designated Record Set. The Plan must generally honor these rights, except in certain circumstances. When the Plan amends PHI, it must communicate the Amendment to other persons to whom it has disclosed the PHI as described in Section 5.03(c). The Plan will require Business Associates to make Designated Record Sets that they maintain available for Amendment requests.

b. Processing a Request

The Plan is responsible for receiving and processing requests for Amendments to PHI. The Plan has assigned this responsibility to Amendment Contact (see Section 10.03). Requests must be submitted on the Request to Amend Form (see Section 10.08(b)) and sent to Amendment Contact. The Plan will develop procedures with Business Associates to coordinate the right to request Amendment of Designated Record Sets in the Business Associates' custody.

Amendment Contact will respond to a Participant's request within sixty (60) days after receipt. If Amendment Contact is unable to respond within this timeframe, he or she will send the Participant written notice that the time period for reviewing the request will be extended for no longer than thirty (30) more days, along with the reasons for the delay and the date by which Amendment Contact expects to address the request.

c. Amending PHI and Notifying Others

If Amendment Contact accepts a request for Amendment, in whole or in part, a copy of Form 10.08(b) indicating that the request has been accepted will be sent to the Participant within the sixty (60) day time frame. Amendment Contact will amend the PHI appropriately, and make reasonable efforts to inform and provide the Amendment to:

- Persons identified by the Participant as having received the PHI that is to be amended; and
- Persons, including Business Associates, who the Plan knows have the PHI that is the subject of the Amendment and who may have relied, or could foreseeably rely, on the information to the detriment of the Participant.

d. Denying an Amendment

If Amendment Contact denies the request for Amendment, in whole or in part, a copy of Form 10.08(b) indicating that the request was denied will be sent to the Participant within the sixty (60) day time frame. Amendment Contact may deny a request to amend a Participant's PHI if

 Copyright © 2015

he or she determines that the PHI:

- Was not created by the Plan (unless the Participant provides a reasonable basis to believe that the creator of the PHI is no longer available to amend the PHI);
- Is not part of the Designated Record Set;
- Is not available for inspection under the HIPAA Privacy Rule; or
- Is accurate and complete.

If Amendment Contact denies the request, it will permit the Participant to submit a statement of disagreement and the basis for the disagreement, limited to five (5) pages. In response, Amendment Contact may provide a rebuttal statement and send a copy to the Participant.

Amendment Contact will attach to each Designated Record Set that is subject to the request a completed copy of Form 10.08(b) (including any attached disagreement statements and rebuttals) indicating the denial of the Amendment request.

When the Plan makes subsequent disclosures of the disputed PHI, a copy of Form 10.08(b) (or a summary of the information included on Form 10.08(b)) will be attached to the PHI disclosed in the following circumstances:

- When the Participant has submitted a statement of disagreement;
- When the Participant has so requested.

e. Documenting Requests

All requests, acceptances, denials, and supporting statements regarding Amendment of PHI will be documented and retained for a period of six (6) years.

f. Citations

45 CFR § 164.526

 Copyright © 2015

5.04 Restricted Use of PHI

a. Participant's Rights

A Participant has the right to request that the Plan restrict the use and disclosure of his or her PHI. In most cases, the Plan is not required to agree to a restriction, but it must abide by an agreed to restriction except in certain circumstances. The Plan will require Business Associates to make PHI that they maintain available for restriction requests.

b. Receiving a Request

The Plan is responsible for processing requests for restricted use of PHI. The Plan has assigned this responsibility to Restriction Contact (see Section 10.03). Requests must be submitted on the Request for Restricted Use Form (see Section 10.08(c)) and sent to Restriction Contact. The Plan will develop procedures with Business Associates to coordinate the restricted use of PHI in the Business Associates' custody.

c. Processing a Request

The Restriction Contact will determine whether to approve or deny restriction requests in consultation with the Privacy Official, as needed.

Out-of-Pocket Payments. The Restriction Contact will agree to restrict disclosure to a health plan for purposes of carrying out payment or health care operations if the request relates to PHI for a health care item or service for which the provider has already been paid in full out-of-pocket. (For example, the Restriction Contact would agree *not* to forward a provider's claim for payment to another health plan for coordination of benefits purposes if the Participant has already paid out of his own pocket the full amount to the provider for the service rendered.)

Procedures. Restriction Contact will provide notice of the approval or denial of the request.

- If approved, a copy of Form 10.08(c) indicating that the request has been approved will be sent to the Participant and to each Business Associate that has access to that Participant's PHI.

- If denied, a copy of Form 10.08(c) indicating that the request has been denied will be sent to the Participant.

Limiting Uses or Disclosures. If Restriction Contact agrees to a restriction, the restriction will not prevent uses or disclosures of PHI to HHS if the agency is investigating the Plan's compliance with the HIPAA Privacy Rule. In addition, Restriction Contact may disregard an agreed-to restriction if disclosing the restricted PHI is necessary to provide emergency Treatment to the Participant. If restricted PHI is disclosed to a health care provider for emergency Treatment, Restriction Contact will request that the health care provider not further

 Copyright © 2015

use or disclose the information.

Terminating a Restriction. An agreed-to restriction may later be terminated in any of the following ways:

- **At the Participant's written request.** A Participant may terminate a restriction by submitting Form 10.08(c) to Restriction Contact. Upon receipt of a signed copy of Form 10.08(c), Restriction Contact will apply the termination of the restriction to all of the Participant's PHI, even if created or received before termination of the restriction.

- **By agreement between the Plan and the Participant.** The Plan may terminate its agreement to a restriction with the Participant's approval. Restriction Contact will send Form 10.08(c) to the Participant (see Section 10.08) for VANDERBILT. Upon receipt of a signed copy of Form 10.08(c), Restriction Contact may apply the termination of the restriction to all of the Participant's PHI, even if created or received before termination of the resolution.

- **By the Plan's unilateral decision.** The Plan may also terminate its agreement to a restriction without the Participant's approval by notifying the Participant in advance of the termination (except for agreements as to PHI relating to items or services paid for through out-of-pocket payments described above). Restriction Contact will send Form 10.08(c) to the Participant for notification purposes. However, when the Participant does not approve the termination, it will apply only with respect to PHI created or received on or after the date Form 10.08(c) is sent.

  If a restriction is terminated, the Plan may use and disclose PHI as permitted by the HIPAA Privacy Rule.

d. Documenting Requests

All restricted use of PHI requests will be documented and retained for a period of six (6) years.

e. Citations

45 CFR § 164.522(a)

 Copyright © 2015

5.05 Confidential Communications

a. Participant's Rights

A Participant has the right to request that the Plan use alternative means or alternative locations to communicate PHI to the Participant. The Plan must accommodate reasonable requests if the Participant clearly states that the disclosure of the PHI by the usual means could endanger the Participant. The Plan will require Business Associates that maintain PHI to reasonably honor a Participant's request for alternative means or locations to communicate the PHI to the Participant.

b. Processing a Request

The Plan is responsible for receiving and processing requests for Confidential Communication of PHI. The Plan has assigned this responsibility to Communications Contact (see Section 10.03). Requests must be submitted on the Request for Confidential Communications Form (see Section 10.08(d)) and sent to Communications Contact. The Plan will develop procedures with Business Associates to coordinate the Confidential Communications of PHI in Business Associates' custody.

Communications Contact will determine whether to approve or deny the request on the basis of its reasonableness. Reasonableness will be determined on the basis of the administrative difficulty in complying with the request and in consultation with the Privacy Official, as needed. If the payment of benefits is affected by this request, the Plan may also deny this request unless the Participant contacts the Communications Contact to discuss alternative payment means.

Communications Contact will provide notice of the decision to approve or deny the request.

- If approved, a copy of Form 10.08(d) indicating that the request has been approved will be sent to the Participant and each Business Associate that has access to that Participant's PHI.

- If denied, a copy of Form 10.08(d) indicating that the request has been denied will be sent to the Participant.

c. Documenting Requests

All requests for Confidential Communication of PHI will be documented and retained for a period of six (6) years.

d. Citations

45 CFR § 164.522(b)

 Copyright © 2015

5.06 Accounting of Nonroutine Disclosures

a. Participant's Rights

A Participant has the right to request an accounting of PHI disclosures made under Section 10.10 and disclosures not otherwise permitted by Section 4. However, an accounting is not available to the Participant in circumstances involving:

- National security or intelligence purposes;
- Correctional institutions or law enforcement officials;
- Limited Data Sets; and
- Disclosures occurring before the compliance date for the Covered Entity.

The Participant can request that the accounting include disclosures made on or after the date that is six (6) years prior to the date of the request.

The Plan will require Business Associates that maintain PHI to reasonably honor a Participant's request for accountings of PHI disclosures.

b. Processing a Request

The Plan is responsible for receiving and processing requests for an accounting of PHI disclosures. The Plan has assigned this responsibility to Disclosure Contact (see Section 10.03). Requests must be submitted on the Request for Accounting of Nonroutine Disclosures Form (see Section 10.08(e)) and sent to Disclosure Contact. The Participant must indicate whether the requested accounting is for disclosures made within the past six (6) years or some shorter time period. The Plan will develop procedures with Business Associates that maintain PHI to coordinate the requests for accounting of PHI disclosures.

Disclosure Contact generally will respond to a request for an accounting within sixty (60) days after receipt. If Disclosure Contact is unable to respond within this timeframe, he or she will send the Participant written notice that the time period for reviewing the request will be extended for no longer than thirty (30) more days, along with the reasons for the delay and the date by which Disclosure Contact expects to address the request.

Disclosure Contact will send a copy of Form 10.08(e) to the Participant, with the accounting of PHI disclosures attached.

 Copyright © 2015

Disclosure Contact will provide a Participant with one accounting in any twelve (12)-month period free of charge. A reasonable fee will be charged for subsequent accountings within the same twelve (12)-month period.

Disclosure Contact may temporarily suspend a Participant's right to receive an accounting of disclosures to:

- A health oversight agency for health oversight purposes; or
- A law enforcement official for law enforcement purposes,

If the agency or official informs Disclosure Contact or the Plan in writing that the accounting would be reasonably likely to impede the agency's activities, and if it indicates the time for which the suspension is required.

Disclosure Contact will suspend a Participant's right to receive an accounting of these disclosures for up to thirty (30) days upon an oral request from the agency or official.

c. Content of the Accounting

Disclosure Contact will include the following information in an accounting of PHI disclosures:

- Date of disclosure;
- Name (and address, if known) of person or entity that received the PHI;
- Brief description of the PHI disclosed; and
- An explanation of the purpose of the disclosure or a copy of the request for disclosure.

The HIPAA Privacy Rule permits an abbreviated accounting of multiple PHI disclosures made to the same person or entity for a single purpose, and of certain disclosures for research purposes. Disclosure Contact will consult with the Privacy Official in deciding to abbreviate an accounting of these types of disclosures.

d. Documenting Requests

All requests for accounting of PHI disclosures will be documented and retained for a period of six (6) years.

e. Citations

45 CFR § 164.528

 Copyright © 2015

6. Risk Management Activities

 Copyright © 2015

6.01 Overview

The Plan must initiate certain risk management activities to ensure compliance with the HIPAA Privacy Rule including:

- Workforce training on the Policies and Procedures for use, disclosure and general treatment of PHI (see Section 6.02);
- Developing a complaint process for individuals to file complaints about the Plan's Policies and Procedures, practices, and compliance with the HIPAA Privacy Rule (see Section 6.03);
- Designing a system of written disciplinary policies and sanctions for workforce members who violate the HIPAA Privacy Rule (see Section 6.04);
- Mitigating damages known to the Plan resulting from improper use or disclosure of PHI (see Section 6.05); and
- Retaining copies of its Policies and Procedures, written communications, and actions or designations (see Section 6.06).

Some of these risk management rules require Covered Entities to design processes affecting workforce members under its control. Since the Plan itself has no workforce, it will comply by requiring Business Associates, Insurers, and relevant VANDERBILT staff to implement the required activity. Sections 6.02 through 6.06 describe the Procedures developed by VANDERBILT.

Additionally, to properly manage its ongoing obligations, the Plan must account for changed VANDERBILT or Plan circumstances and for regulatory changes. Section 6.07 contains guidelines for revising the Plan's Procedures.

 Copyright © 2015

6.02 Training

HIPAA generally requires Covered Entities to provide training to all current and future workforce members under their direct control on the use, disclosure, and general treatment of PHI. Since the Plan itself has no workforce members. VANDERBILT will train and periodically retrain its relevant workforce members to ensure that it meets its obligations under this Manual (including limiting the use and disclosure of PHI as required under Section 4). The Privacy Official or his or her designee will coordinate the training. Business Associates and Insurers will separately engage in training activities as needed to ensure they meet their responsibilities under the HIPAA Privacy Rule and Business Associate Agreements (as applicable).

a. When Training will Occur

Workforce members of VANDERBILT who will have access to PHI will receive privacy training as part of their initial training. Workforce members who change employment positions or functional roles will receive new privacy training, as relevant, at the time of the change. VANDERBILT will also retrain appropriate members of the workforce after a material change in the Plan's Policies and Procedures. The retraining will occur within a reasonable time after the Plan changes its Policies and Procedures.

b. Contents of Training

Workforce training on the use and disclosure of PHI will address the protection, permissible disclosures, and general treatment of PHI.

c. Specialized Training Due to Job Descriptions

Members of the workforce who require specialized training due to their particular job function, rank, exposure to PHI or discipline, will be trained accordingly.

d. Documentation

Documentation of privacy training will be maintained by the Privacy Official for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

e. Citations

45 CFR § 164.530(b)

 Copyright © 2015

6.03 Complaints

The Plan is required to create a process for persons to file complaints about the Plan's Policies and Procedures, practices, and compliance with the HIPAA Privacy Rule. This Section describes the complaint process for self-funded Plan benefits. Insurers will develop procedures to process complaints about insured benefits as required under the HIPAA Privacy Rule.

a. Filing Complaints

Complaints should be filed by contacting Complaint Manager and include a description of the nature of the particular complaint.

b. Processing Complaints and Complaint Resolution

Complaint Manager will review the complaint, address the situation, consult with the proper individuals (if necessary), and attempt to come to an appropriate resolution of the complaint.

The resolution will depend on the particular facts and circumstances of the complaint. Examples of complaint resolution include:

- Educating the individual about the Plan's Policies and Procedures or practices;
- Coordinating with the Breach Contact regarding complaints alleging use or disclosure of PHI in violation of the Plan's Policies and Procedures;
- Implementing changes in the Plan's Policies and Procedures or practices;
- Providing additional training for workforce members on the Plan's Policies and Procedures, the HIPAA Privacy Rule, or other applicable laws or regulations;
- Discussing a complaint with the relevant parties and, if necessary, imposing sanctions on individuals who violate the Plan's Policies and Procedures or the HIPAA Privacy Rule; and
- Issuing new workforce communication materials or a revised Privacy Notice regarding the Plan's Policies and Procedures.

If, at any time, an individual wants to know the status of his or her complaint, he or she should contact Complaint Manager.

 Copyright © 2015

Once Complaint Manager has resolved a complaint, he or she will contact the individual who filed the complaint and discuss the resolution and/or send a written or electronic communication to the individual who filed the complaint explaining the resolution.

c. Documentation

The Plan will maintain a record of the complaints and a brief explanation of their resolution, if any, for a period of six (6) years.

d. Citations

45 CFR § 164.530(d)

Copyright © 2015

6.04 Sanctions

Covered Entities are required to design a system of written disciplinary policies and sanctions for workforce members who violate the HIPAA Privacy Rule. Since the Plan itself has no workforce members the Plan will work with VANDERBILT to implement procedures to apply sanctions against VANDERBILT's workforce members who violate the Plan's Policies and Procedures or the HIPAA Privacy Rule. Business Associates and Insurers will take whatever steps are required to ensure their compliance with the HIPAA Privacy Rule and Business Associate Agreements (as applicable).

a. Determining Sanctions

The Plan will determine a sanction at the time of a violation and will base the sanction on the nature of the violation and will work with VANDERBILT to apply the sanction Factors taken into account will include the severity of the violation, whether it was intentional or unintentional, and whether it indicated a pattern or practice of improper use or disclosure of PHI. Examples of possible sanctions include:

- Required additional training;
- Verbal warnings;
- Written warnings;
- Probationary periods; and
- Termination of employment.

The Plan will not apply sanctions against workforce members who refuse to follow a Policy or Procedure that they believe, in good faith, violates the HIPAA Privacy Rule, if the refusal is reasonable and does not involve a disclosure of PHI. In addition, the Plan will not apply sanctions against workforce members who file a complaint with any entity about a privacy violation.

b. Documentation

The Plan will document in writing (or in an electronic medium) all sanctions it applies. The Plan will retain the documentation of any sanctions it applies for six (6) years.

c. Citations

45 CFR § 164.530(e)

 Copyright © 2015

6.05 Mitigation of PHI Breaches

The Plan is required to mitigate any harmful effects that it knows have resulted from improper access, use, or disclosure (a breach) of PHI in violation of the Plan's Policies and Procedures or the HIPAA Privacy Rule. To meet this obligation, the Plan will coordinate with and require Business Associates to mitigate, to the extent practicable, any harmful effects from breaches of PHI known to them. Insurers are also required to mitigate such harmful effects under HIPAA.

The Plan's Breach Contact will conduct, or direct others in the performance of, the mitigation activities.

a. Investigating Reported Breaches Originating from VANDERBILT

The Plan's Breach Contact (or his or her designee) will review all Forms 10.09(a) submitted for evaluation and timely take appropriate steps to learn relevant facts about the incident and apply corrective measures, including:

- Verify there was a problematic access, use or disclosure of PHI and confirm that no exception under the Privacy Rule would permit it;
- Interview relevant workforce members to learn about circumstances surrounding the incident;
- Review manual logs, electronic logs, closed circuit television tapes and/or other feasible references to determine the source(s) of the breach if that is unknown;
- Conclude whether an impermissible access, use, or disclosure occurred (or is reasonably believed to have occurred), how it occurred and, in coordination with the Privacy Official and/or Security Official, identify corrective steps needed to prevent a similar incident from reoccurring (which may include additional training for workforce members and applying sanctions against workforce members in accordance with Section 6.04); and
- Begin completion of the Breach Incident Log (Form 10.09(b)) capturing the above facts and conclusions.

b. Assessing Whether the Incident Requires VANDERBILT *to Send Breach Notices*

The Plan has an affirmative duty under HIPAA's Breach Notice Rule to send affected individuals a notice about impermissible accesses, uses and disclosures of their PHI unless an exception to the breach notice requirement applies.

The Breach Contact (or his or her designee) will initially assess whether an exception to the notice duty applies to the incident under the Breach Notice Rule, including:

 Copyright © 2015

- The affected data was in a "secured" format at the time of the incident (that is, a format deemed by HHS to make the PHI unusable, unreadable, or indecipherable to unauthorized persons – as outlined in then-applicable HHS guidelines found at http://www.hhs.gov/ocr/privacy or other successor website);

- The incident consisted of the unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of the Plan or a Business Associate, and the acquisition, access or use was made in good faith and within the scope of authority and did not result in further use or disclosure that is disallowed under the Privacy Rule;

- The incident consisted of inadvertent disclosure by a person authorized to access PHI at the Plan or its Business Associate to another person authorized to access PHI at the Plan or a Business Associate in the organized healthcare arrangement in which the Plan participates, and the PHI was not further used or disclosed in a manner disallowed under the Privacy Rule;

- The Plan has a good faith belief that the unauthorized person(s) to whom the disclosure was made would not reasonably have been able to retain the information; or

- The Plan has reasonably determined that there is a low probability that the PHI has been compromised. In deciding whether there is a low probability that the PHI has been compromised the Plan must take the following into account: the type of data elements involved and whether they could be used to identify a person; any information the Plan obtains on whether the data was actually viewed (for example through a forensic review of the data); whether the Plan was able to mitigate the risk the PHI was compromised (for example by asking the unauthorized person to destroy or return the information); and the nature of the unauthorized person who had access to the PHI.

The Plan will make reasonable efforts to document its determination of whether or not a breach has occurred.

If one or more exceptions to the breach notice obligation applies under this Section 6.05(b), VANDERBILT will consider whether notice to some or all of the potentially affected individuals is nevertheless appropriate. If so, the Breach Contact (or his or her designee) will take steps to notify such individuals but will *not* be obligated to follow the specific timelines or steps outlined in Sections 6.05(c) through (e) below. Additionally, the Breach Contact (or his or her designee) will finish filling out the Breach Incident Log (see Form 10.09(b)) related to the incident.

If no exception applies, the Breach Contact will conduct, or direct others in the performance of, the procedures outlined in Sections 6.05(c) through (e) below.

In any case, VANDERBILT also will take into account any notice obligation that applies under relevant state privacy law, except to the extent that such state law is contrary to the HIPAA Breach Notice Rule; in that case, compliance with the Breach Notice Rule will prevail.

 Copyright © 2015

c. Preparing Breach Notices

If the Breach Notice Rule requires that VANDERBILT send notice to affected individuals, the Breach Contact (or his or her designee) will oversee the preparation of the notice, which will include determining whether receiving advice of counsel is necessary or prudent in the notice development.

Any notice drafted to satisfy the Breach Notice Rule will be written in plain language and will cover at least the following elements of information:

Breach Notice Content

Required Element	Example
Brief description of what happened, including the date of breach and (if known) the date of discovery)	✓ on or around July 31, 2010, [entity's] Seattle offices experienced a break-in and theft of some office equipment, including several desktop computers ✓ the incident was discovered when staff returned for regular working hours on August 2, 2010 ✓ some of the missing desktops contained information necessary for administration of the [Name of Plan], in which you are enrolled as a [Name of Employer] employee
Types of PHI involved (e.g., name, SSN, DOB, home address, account numbers, diagnosis information)	✓ types of information contained in the missing computers includes Plan enrollees' full names, Social Security numbers, and home addresses
Steps individuals should take to protect themselves from potential harm resulting from the breach	✓ contact your financial institution to alert them to the possible theft of this personal information ✓ contact the free government *[free gov't service by website/address]* ✓ obtain credit monitoring services from a credit bureau to continually receive information about your credit status and observe specific activity in your name
Brief description of what VANDERBILT is doing to investigate the breach, mitigate harm to individuals, and protect against further incidents	✓ immediately filed a police report with the appropriate authorities and cooperated in the police investigation of the theft ✓ actively monitoring the progress of the police investigation ✓ will make all reasonable efforts to recover the missing computers ✓ installed encryption protections on all portable devices that contain PHI

d. Distributing Breach Notices

Individual HIPAA breach notices and, if applicable, media notices, will be sent without unreasonable delay and in no case later than 60 calendar days after discovery of the incident. *In addition to* taking the below steps, if the Plan determines during the investigation of the incident that possible misuse of

 Copyright © 2015

the PHI may be imminent, the Plan may take more urgent action to contact the affected individuals, such as by telephone or other immediate medium.

In accordance with the Breach Notice Rule, VANDERBILT will take the following applicable steps to distribute the breach notice:

Individual Notice

- Notice will be sent by first-class mail to the individual's last-known address (or by e-mail if the affected individual agrees to electronic notice and the agreement hasn't been withdrawn);
- If the affected person is deceased, notice will be sent by first-class mail to the person's next-of-kin or personal representative, but only if VANDERBILT has their contact information;
- If the contact information for the affected individual is out of date, VANDERBILT will send a substitute form of notice reasonably calculated to reach the person, which could be by e-mail message, telephone, or other means (except that no substitute form of contact is necessary if the unreachable person is the next-of-kin or personal representative);
- If there are *ten or more* affected people who cannot be mailed the written notice due to insufficient or outdated contact information (taking into account the number whose notice was returned as undeliverable), VANDERBILT will either
  - conspicuously post a hyperlink to the substitute notice on the Plan's website homepage for at least 90 days, *or*
  - provide the notice in major print or broadcast media where the affected individuals likely reside, *and*

  the substitute notice will include a toll-free telephone number (active for at least 90 days) for individuals to contact the Plan to learn if their PHI was involved in the breach incident.

Media Notice

- If the breach incident affects the PHI of more than 500 residents of a State then, *in addition to* taking the individual notice steps above, VANDERBILT will direct a press release to prominent media outlets serving that State (or smaller area where the affected people reside), which will cover the same topics required for the individual notice.

Additionally, the Breach Contact (or his or her designee) will finish filling out the Breach Incident Log (Form 10.09(b)) related to the incident.

e. Reporting Breach Incidents to HHS

The Breach Contact (or his or her designee) will notify HHS of each breach incident entered in the Plan's Breach Incident Log (Form 10.09(b)) for which no notice exception is available under the Breach Notice Rule. The report will be made by visiting the applicable HHS web site and filling out and electronically submitting the agency's breach report form. If a breach affects 500 or more individuals, the Plan will report to HHS at the same time that the Plan distributes the individual notices to affected people. If a breach affects fewer than 500 individuals, the Plan may

 Copyright © 2015

notify HHS of such breaches on an annual basis, but no later than 60 days after the end of the calendar year in which the breach occurred.

f. Mitigation Steps for Breaches Originating from a Business Associate

All Business Associates must report to the Plan any breaches of PHI as soon as possible after discovery. The Plan will coordinate with each Business Associate to ensure that the above applicable steps are executed with respect to each breach incident. The Plan may decide to require the Business Associate to undertake relevant notification and mitigation steps. In some cases, the Business Associate agreement may include certain notification and/or mitigation steps as contractual obligations of the Business Associate.

g. Documentation

The Plan will maintain all Breach Incident Logs for a period of six (6) years.

h. Citations

45 CFR § 164.530(f)
45 CFR § 164.400 - 408

 Copyright © 2015

6.06 Document Retention

The Plan must retain copies of its Policies and Procedures and all communications that the HIPAA Privacy Rule requires to be in writing. The Plan must also retain records of actions or designations that the HIPAA Privacy Rule requires to be documented. Materials can be maintained in written or electronic form. They must be retained for six (6) years from the date of their creation or when they were last in effect (whichever is later).

Business Associates and Insurers will retain documents in their possession as required by the HIPAA Privacy Rule and Business Associate Agreements.

a. Document Retention Checklists

The following are checklists of materials that VANDERBILT will retain under this rule:

Documents	
☐ Privacy Policies and Procedures (this Manual) ☐ Authorizations ☐ Plan Amendments ☐ Plan Amendment certifications ☐ Business Associate Agreements ☐ Notices of Privacy Practices ☐ Documentation that training has been provided to employees	☐ Information in Designated Record Set to which Participants and similar persons have access (see Section 5.02)

Key person identification	
☐ Name of Privacy Official ☐ Name of contact person or office responsible for receiving complaints and providing additional privacy information ☐ Titles of persons or offices responsible for receiving and processing requests for access to their PHI	☐ Titles of persons or offices responsible for receiving and processing requests to amend PHI ☐ Titles of persons or offices responsible for receiving and processing requests for an accounting of nonroutine disclosures made without Authorization, such as disclosures legally required or made for public health, law enforcement, judicial, and similar purposes

 Copyright © 2015

Other materials relating to particular actions by the Plan	
☐ Complaints about the HIPAA Privacy Rule or this Manual and their disposition, if any	☐ Conclusion and supporting analysis from an expert that health information is deidentified
☐ Documentation of sanctions applied to employees for not complying with the HIPAA Privacy Rule, if any	☐ Copy of disclosure requests (or if made orally, statements describing the disclosures' purpose)
☐ Notices that deny a person's access to PHI	☐ Court orders, grand jury subpoenas , etc., where disclosure is required by law
☐ Notices that delay a person's access to PHI	☐ Written statements in connection with disclosures needed for other judicial/ administrative processes, where the disclosure is not mandated by court order
☐ Notices that explain whether the Plan will overturn a decision to deny a person access to PHI	☐ Institutional or privacy board approvals for research-related disclosures
☐ Notices that deny a person's request to amend PHI	☐ Copies of written accountings
☐ Notices that delay amendments to PHI	☐ Plan's notice terminating a restriction on uses or disclosures of PHI previously agreed to by the Plan
☐ Statements of persons disagreeing with the Plan's decision to deny a request to amend PHI and any rebuttals of the statements	☐ Person's agreement or request to terminate a restriction on uses or disclosures of PHI previously agreed to by the Plan
☐ Disclosures of PHI for which a person is entitled to an accounting	
☐ Written statements or other documentation in support of verifications made prior to disclosures	
☐ Written statements by agencies or officials supporting suspension of an accounting of PHI disclosures (including oral statements documented by the Plan)	

b. Citations

45 CFR § 164.530(j)

Copyright © 2015

6.07 Guidelines for Policy and Procedure Changes

In order for the Policies and Procedures to remain current, the Plan must consider modifying the Policies and Procedures to account for changed circumstances. Such changes may involve, for example, amendments to the HIPAA Privacy Rule, adoption of a new group health plan, or termination of a Business Associate, among others.

The process for Policy and Procedure modification involves the following steps:

- Monitor changes that may impact the Policies and Procedures
- Assess the impact on the Policies and Procedures
- Modify the Policies and Procedures, if appropriate
- Distribute (and, if appropriate, provide training on) modified Policies and Procedures

The events for which a HIPAA impact assessment should be conducted include, but are not limited to, those described in the table beginning on the following page. The table also identifies the types of actions recommended to address the respective events. Each event will require specific review to determine an appropriate action plan.

The Privacy Official will generally be responsible for coordination of the Policies and Procedures under the HIPAA Privacy Rule. Accordingly, the recommended actions in the following table will typically be undertaken either directly by the Privacy Official or, at the direction of the Privacy Official, by others such as plan administrative staff, internal legal counsel, and/or external advisors.

Copyright © 2015

Event	Recommended Action(s)
Change in VANDERBILT **Operations**: • New staff members • New technology • New operating procedures	• Monitor and update any changes in HIPAA Privacy Complaint Manager (and other Contacts) listed in Section 10.03. • Update and refer to Section 10.02 in the event of any change involving the Privacy Official. • Monitor changes in technology and business operating procedures involving processes for handling PHI under the Policies and Procedures. In particular, changes should be reviewed for any effect on Policies and Procedures in Sections 3 and 4. • Implement training appropriate to the level of any revisions in Policies and Procedures resulting from staffing, technology or operations changes. • Revise (and distribute revised) Notice of Privacy Practices, if applicable. (See Section 7.02(c) for additional information.)
Rule Change: Changes in the HIPAA Privacy Rule or related rules (for example, the final security rule). Changes may occur in statutes, regulations, agency guidance, or case law.	• Monitor developments changing the applicable rules. • Identify specific Policies and Procedures affected by the development. • Assess need for modifications to the Policies and Procedures. • Revise Policies and Procedures – including legal documents referenced in Section 7 and Participant forms referenced in Section 5 – as appropriate. • Distribute revised Policies and Procedures and training materials. • If applicable, distribute revised HIPAA Privacy Notice and Sponsor Certification. • If applicable, negotiate modifications to Business Associate agreements and other vendor contracts.
Business Associate Addition: Adding a new Business Associate. Change may occur at renewal, mid-term (for example, replacement of prior vendor), or by reason of a merger or other transaction affecting an existing Business Associate.	• Monitor circumstances leading to addition of Business Associate. If possible, include model Business Associate agreement in any applicable RFP specifications. • Negotiate and customize the Business Associate agreement and present it for execution to the vendor. • Amend Section 10.04b (“Log of Business Associate Agreements”) and any other documents referring to the Business Associate. • If change coincides with a change in any Plan, refer to guidelines below on “Termination of Group Health Plan” or “Addition or Name Change in Group Health Plan” as applicable.

 Copyright © 2015

Event	Recommended Action(s)
Business Associate Termination: Terminating an existing Business Associate. Change may occur at renewal, mid-term (for example, a termination for performance failure), or by reason of a merger or other transaction affecting the Business Associate.	• Monitor circumstances requiring termination of Business Associate. • Clarify Plan's needs and, if necessary, negotiate termination provisions with the Business Associate concerning issues such as transfer of data, and continued HIPAA contact responsibilities delegated to the Business Associate. In particular, will vendor retain any PHI? If so, who are the contacts for continued access to PHI? Consider agents and subcontractors of Business Associate. • Amend Section 10.04b ("Log of Business Associate Agreements") and any other documents referring to the Business Associate. • If change coincides with a change in any Plan, refer to guidelines below on "Termination of Group Health Plan" or "Addition or Name Change in Group Health Plan" as applicable.
Insurer Addition: Adding a health plan insurer.	• Monitor circumstances leading to addition of an insurer. • Obtain and preserve contact information for purposes of referring future PHI requests. • Review and modify any references to the insurer in the Policies and Procedures (for example, references in Section 10.05 and the Notice of Privacy Practices), as appropriate. • Furnish Plan Sponsor Certification, as appropriate (if PHI will be obtained from the insurer). • Obtain copy of insurer's Notice of Privacy Practices if making it available on request to Participants.
Insurer Termination or Policy Revision: Terminating a health plan insurer, or accepting a revised group insurance policy or contract by existing insurer.	• Monitor circumstances requiring termination of the insurer or acceptance of a revised group insurance policy or contract. • Update and preserve contact information for purposes of referring requests for PHI maintained by insurer under a prior policy or contract. • Review and modify any references to the insurer in the Policies and Procedures (for example, references in Section 10.05 and the Notice of Privacy Practices), as appropriate. (Retain listing but mark as "former" carrier, if appropriate.)

 Copyright © 2015

Event	Recommended Action(s)
Addition or Name Change in Group Health Plan: Adding a health plan, or changing the current Plan name.	• Monitor addition of a health plan potentially subject to the HIPAA Privacy Rule (or of a change in the name of an existing Plan). • Determine if new plan is subject to the HIPAA Privacy Rule, and whether it is a separate group health plan or a component of an existing Plan. • Determine application of "organized health care arrangement" to all Plans, including modifications to Policies and Procedures and use of joint Notice of Privacy Practices. • Amend Section 10.01 ("Covered Plans") and any other documents or forms referring to the Plans, as appropriate. • Refer to guidelines above on "Business Associate Addition" or "Insurer Addition", as applicable. • Consider if changes in personnel are also implicated.
Termination in Group Health Plan: Terminating a Plan or a component Plan subject to the HIPAA Privacy Rule.	• Monitor circumstances leading to deletion of a Plan subject to the HIPAA Privacy Rule. • Determine impact on application of "organized health care arrangement" to all Plans, including modifications to Policies and Procedures and use of joint Notice of Privacy Practices. • Amend Section 10.01 ("Covered Plans") and any other documents or forms referring to the Plans, as appropriate. • Refer to guidelines above on "Business Associate Termination" or "Insurer Termination or Policy Revision" as applicable. • Consider if changes in personnel also implicated. • Identify and preserve contact information for PHI maintained in connection with the terminated Plan.
Acquisitions by VANDERBILT: Adding a subsidiary.	• Determine if the added subsidiary sponsors a group health plan. • Determine if new plan is subject to the HIPAA Privacy Rule, and whether it is a separate group health plan or will become a component of an existing Plan. • Determine application of: (i) "organized health care arrangement" status to all Plans (this may be appropriate if the same VANDERBILT entity is the sponsor of all the Plans), or (ii) "affiliated covered entity" status to all Plans (this may be appropriate if the new subsidiary will continue to be the sponsor of its group health plan). Review Policies and Procedures, including the Notice of Privacy Practices, for corresponding changes. • Amend Section 10.01 ("Covered Plans") and any other documents or forms referring to the Plans, as appropriate. • Refer to guidelines above on "Business Associate Addition" or "Insurer Addition" as applicable. • Consider if changes in personnel are also implicated.

 Copyright © 2015

Event	Recommended Action(s)
Divestitures by VANDERBILT: Terminating a subsidiary.	• Determine if the terminating subsidiary sponsors (or is the sole participating entity in) a Plan covered by the Policies and Procedures. • Verify whether the subsidiary Plan is a separate group health plan or a component of another Plan. • Determine any impact on the application of: (i) "organized health care arrangement" status to all Plans (this may be an issue if the same VANDERBILT entity is the sponsor of two or more Plans), or (ii) "affiliated covered entity" status to all Plans (this may be an issue if the terminating subsidiary sponsored its own Plan separate from Plans sponsored by another VANDERBILT entity). Review Policies and Procedures, including the Notice of Privacy Practices, for corresponding changes. • Amend Section 10.01 ("Covered Plans") and any other documents or forms referring to the Plans, as appropriate. • Refer to guidelines above on "Business Associate Termination" or "Insurer Termination or Policy Revision" as applicable. • Consider if changes in personnel are also implicated.

 Copyright © 2015

7. Required Legal Documents

 Copyright © 2015

7.01 Overview

The HIPAA Privacy Rule requires Covered Entities to use specific documents to accomplish certain tasks.

- A Privacy Notice describes the Plan's practices concerning its uses and disclosures of PHI and informs Participants of their rights and of the Plan's legal duties, with respect to PHI (see Section 7.02);

- An Amendment to the Plan document describes the Plan's permitted uses and disclosures of PHI (see Section 7.03);

- A plan sponsor certification certifies that the Plan Sponsor has adopted the Plan Amendment and agrees to the restrictions on the uses and disclosures of PHI (see Section 7.04);

- A Business Associate Agreement describes the permitted uses and disclosures of PHI by the Business Associate (see Section 7.05); and

- A Participant's Authorization permits the Plan to use and disclose the Participant's PHI for purposes not otherwise permitted or required by the HIPAA Privacy Rule (see Section 7.06).

 Copyright © 2015

7.02 Privacy Notice

VANDERBILT will provide a Privacy Notice in Section 10.07 to satisfy the notice obligation for the Plan's self-funded benefits. Each health insurance issuer or HMO will provide its own Privacy Notice to Participants who receive insured Plan benefits, as required by the HIPAA Privacy Rule. If VANDERBILT (or a Business Associate) receives PHI from a health insurance issuer or HMO to perform Plan administration activities for insured Plan benefits, VANDERBILT will provide the Privacy Notice to Participants in the insured plan upon request.

a. Identifying the Recipients

VANDERBILT will provide the Privacy Notice (see Section 10.07) to new enrollees under a self-funded Plan benefit at the time of enrollment. VANDERBILT will not provide a separate Privacy Notice to spouses or dependents, except for qualified beneficiaries who made independent COBRA elections (e.g., following a divorce or the death of an employee).

In addition, VANDERBILT will provide the Privacy Notice to Business Associates and workforce members who perform Plan functions, during their initial training and annually thereafter.

b. Distributing the Notice

VANDERBILT will provide the Privacy Notice by in-hand delivery or first-class mail.

VANDERBILT also may provide the Notice by e-mail, if the Participant has agreed to electronic notice and the agreement has not been withdrawn. VANDERBILT will provide a paper copy of the Notice if it knows that email transmission failed.

VANDERBILT will prominently post the Notice on any web sites that it maintains that provide information about the Plan's services or benefits.

c. Revising the Notice

VANDERBILT will revise the Privacy Notice if its terms are affected by a change to the Plan's Policies and Procedures.

If the change is material (as determined by the Privacy Official), VANDERBILT will post the Revised Notice on its web site by the effective date of the material change and provide the revised Privacy Notice to Participants covered under a self-funded Plan benefit in its next annual mailing.

 Copyright © 2015

d. Informing Participants of the Availability of the Notice

Once every three (3) years, VANDERBILT will inform all Participants of the Privacy Notice's availability and how to obtain a copy.

e. Documenting Notices

All Privacy Notices will be documented and retained for a period of six (6) years from the date of creation or when last in effect, whichever is later.

f. Citations

45 CFR § 164.520(c) – (e)

Copyright © 2015

7.03 Amendment to Plan Documents

The HIPAA Privacy Rule permits the Plan to share PHI with VANDERBILT after VANDERBILT has amended its Plan documents, as described. VANDERBILT must restrict its use of the PHI to Payment and Health Care Operations activities.

a. Required Plan Amendments

VANDERBILT will amend its Plan Documents (see Section 10.06(a)) to include provisions that:

- Describe VANDERBILT's permitted uses and disclosures of PHI;
- Provide that the Plan can disclose PHI to VANDERBILT only upon receipt of a written certification from VANDERBILT that the Plan Documents have been amended to include specific restrictions on the use and disclosure of PHI and that VANDERBILT has agreed to those restrictions; and
- Provide adequate firewalls, such as identifying the employees (by name or by function) who will have access to PHI, restricting access solely to the identified employees for Plan administration functions, and providing a mechanism for resolving issues of noncompliance.

b. Documenting Plan Amendments

VANDERBILT will retain the amended Plan Documents for a period of at least six (6) years from the date when last in effect.

c. Citations

45 CFR § 164.504(f)(2)

 Copyright © 2015

7.04 Plan Sponsor Certifications

The HIPAA Privacy Rule requires VANDERBILT to certify to the Plan that it has amended its Plan documents in order for the Plan to share PHI with VANDERBILT. The Plan will disclose PHI to VANDERBILT only after VANDERBILT provides the Plan with that written certification.

a. Written Certification Requirements

VANDERBILT's written certification (see Section 10.06(b)) provides that VANDERBILT will take the following actions:

Required elements of VANDERBILT's **written certification**
• Not use or further disclose PHI other than as permitted or required by the Plan documents or as required by law; • Ensure that any vendors or agents to whom VANDERBILT provides PHI agree to the same restrictions; • Not use or disclose the PHI for employment-related actions or in connection with any other benefit program of VANDERBILT; • Report to the Plan any use or disclosure of which VANDERBILT becomes aware that is inconsistent with the Plan documents or the HIPAA Privacy Rule; • Make PHI accessible to individuals in accordance with Section 4.02; • Allow individuals to amend their information in accordance with Section 4.03; • Provide an accounting of its disclosures in accordance with Section 4.06; • Make its practices available to HHS for determining compliance; • Return and destroy all PHI when no longer needed, if feasible; and • Ensure that adequate separation exists between VANDERBILT's Plan administration activities and all other activities.

b. Documenting Certifications

All certifications will be retained for a period of six (6) years.

Copyright © 2015

c. Citations

45 CFR § 164.504(f)(2)(ii)

Copyright © 2015

7.05 Business Associate Agreements

The HIPAA Privacy Rule requires each Business Associate of the Plan to enter into a written contract (a Business Associate Agreement) with the Plan before the Plan can disclose PHI to it, except as indicated below. The Business Associate must also enter into a Business Associate Agreement with each of its subcontractors that will be performing a task on behalf of the Business Associate, if that task relates to the use and disclosure of the PHI of participants and beneficiaries of the Plan. The Business Associate (and it subcontractors) can use and disclose PHI only for the purposes provided in the Business Associate Agreement. The Privacy Official will monitor how PHI maintained by the Business Associate is handled at the termination of the Business Associate Agreement and will, while the agreement is in force, act upon complaints of privacy violations and breaches.

a. Identifying Business Associates

VANDERBILT will determine which service providers are Business Associates. The log of Business Associate Agreements is at Section 10.04.

b. Signing Business Associate Agreements

The Plan will require each Business Associate to sign a Business Associate Agreement (see Section 10.04) or a contract that contains the required terms, as determined by the Privacy Official. That Business Associate Agreement will require each Business Associate to sign a Business Associate Agreement with each vendor that the Business Associate utilizes who will use or disclose PHI of Plan participants and beneficiaries.

c. 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 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.

 Copyright © 2015

d. 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.

e. Citations

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

Copyright © 2015

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

VANDERBILT or Business Associate will provide an Authorization Form (see Section 10.08(f)) to a Participant who requests that his or her PHI be disclosed to a third party (other than a personal representative).

VANDERBILT or Business Associate will provide each Participant with an Authorization Form if VANDERBILT or Business Associate 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

 Copyright © 2015

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

Copyright © 2015

8. Definitions

Copyright © 2015

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.

Breach Notice Rule: Regulations that mandate notice to individuals in some cases if their PHI is improperly accessed, used, or disclosed, as well as a report to HHS of such incidents. Media notice may also be required. The notice/report contents, timing, and distribution requirements are prescribed by the Breach Notice Rule.

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 person or entity that transmits PHI to a Covered Entity (or its Business Associate) and routinely requiring access to that PHI may also be a Business Associate. Examples of such entities include health information exchange organizations, regional health information organizations and e-prescribing gateways. Vendors that contract with Covered Entities offering certain personal health records to individuals may also be considered Business Associates. 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. Subcontractors of Business Associates performing functions utilizing PHI must enter Business Associate Agreements of the "first tier" Business Associate.

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).

Deidentification: 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 Deidentification 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

 Copyright © 2015

(see Section 5.02).

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

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, and 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 affect how group health plans and their vendors use, disclose, transmit, and secure health information. The administrative simplification rules include: privacy protections, rules for transmission of electronic health care data (electronic data interchange or "EDI"), and security standards for health information. The "HIPAA Privacy Rule" refers to the 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.

Limited Data Set: A limited data set is PHI that **excludes** all of the following direct identifiers: Names; postal address information, except town or city, state, and zip code; telephone numbers; fax numbers; e-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 URLs; IP addresses; biometric identifiers, including finger and voice prints; and full-face photographic images and any comparable images.

 Copyright © 2015

Marketing: An arrangement between a Covered Entity and any other entity whereby the Covered Entity discloses PHI for the other entity or its affiliate, in exchange for direct or indirect remuneration, to make a communication about its own product or service that encourages purchase or use of that product or service. Marketing is also 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.

However, the exceptions described above will not be excluded from the definition of Marketing if the Covered Entity or its Business Associate receives or has received direct or indirect payment in exchange for making such communication , except where (i) such communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication and any payment received by such Covered Entity in exchange for making a communication is a reasonable amount; (ii) the communication is made by the Covered Entity or its Business Associate and the Covered Entity (or the Business Associate) obtains from the recipient of the communication a valid Authorization for that communication; or (iii) the communication is made by a Business Associate on behalf of the Covered Entity and the communication is consistent with the written Business Associate Agreement between the Covered Entity and the Business Associate, and the Business Associate is not receiving direct or indirect payment from a third party for making the communication.

Minimum Necessary*:* To the extent practical, Covered Entities are expected to make a reasonable effort to limit uses and disclosures of, and requests for, PHI to the minimum amount of information needed to support the purpose of the use, disclosure, or request. The Minimum Necessary amount of PHI used, disclosed or requested by the Plan should be restricted to the amount of PHI needed to accomplish the intended purpose of the transaction.

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

 Copyright © 2015

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 and Breach Notice 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, including genetic 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.

 Copyright © 2015

 Copyright © 2015

9. HIPAA Resources

The complete suite of HIPAA Administrative Simplification Regulations can be found at 45 CFR Parts 160, 162, and 164, and includes:

- Transactions and Code Set Standards
- Identifier Standards
- Privacy Rule
- Security Rule
- Enforcement Rule
- Breach Notification Rule

The Department of Health and Human Services Office of Civil Rights HIPAA privacy website

Copyright © 2015