Vanderbilt University

# HIPAA Privacy Manual

As prepared by

Mercer

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.

## Table of Contents

# 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.*

***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).*

# 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. Notwithstanding any other statement in this Manual, VANDERBILT will comply with the requirements published in 89 FR 32976, which are effective beginning December 23, 2024, and further described in Section 4.08.

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.

# 3. Safeguards

## 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.

# 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.<br>• Limit the number of photocopies made of PHI.<br>• 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.<br>• 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.<br>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.<br>• 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).<br>• Encrypt e-mail set outside organization that includes PHI.<br>• Require password entry each time an employee accesses the e-mail system.<br>• Use "locking" screensavers to limit access.<br>• Maintain and periodically update network monitoring software, including intrusion detection and reporting. |

| Protected information | Protection procedures |
|---|---|
| | • Maintain and periodically update systems for backing up data and contingency plans for data recovery in the event of a disaster.<br>• Maintain and periodically update systems for tracking access and changes to data.<br>• Periodically review the process for handling system maintenance and the hardware/software acquisition process.<br>• Maintain and periodically update virus software and protection processes.<br>• Maintain and periodically review procedures for ending data access for staff (e.g., after they terminate employment).<br>• Follow other company IT guidelines regarding electronic data.<br>• Limit remote access to systems to secure methods |
| Facsimiles | • Ensure that fax machines used foe plan administration are not located in publicly accessible areas<br>• Develop fax coversheet including confidentiality statement and warning about releasing data.<br>• Limit faxing of PHI to urgent information.<br>• Notify the receiver in advance that VANDERBILT is sending a fax with PHI so he or she can retrieve it immediately.<br>• 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.<br>• Verify the identity of individuals on the phone (see Section 3.03).<br>• 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<br>• Limit voicemail messages, or messages left for other individuals, to high-level information to ensure no one else could overhear PHI. |

## 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.

### a. Citations

45 CFR § 164.514(h)

# 4. Uses and Disclosures

## 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

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

# 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.<br>• 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.

| 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<br>• Social Security numbers<br>• Full face photographic and any comparable images<br>• Telephone numbers<br>• 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)<br>• Device identifiers and serial numbers<br>• Web Universal Resource Locators (URLs)<br>• Fax numbers<br>• E-mail address<br>• Medical record number<br>• Any other unique identifying numbers, or characteristics, or codes, including particular subsidiaries, divisions, or work locations | • Health plan beneficiary numbers<br>• Account numbers<br>• Certificate/license numbers<br>• Internet Protocol (IP) address numbers<br>• Biometric identifiers (e.g., finger, iris, or voice prints)<br>• 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)

# 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.

## 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.<br>• Health care providers involved with treating the Participant<br>• Business Associates involved in the initial benefit determination.<br>• 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:<br>– copies of the denial letter and appeal decision letter.<br>– documents submitted by the claimant, health care providers, etc.<br>– 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."<br>• Electronic records will be retained consistent with the Plan's HIPAA Security Manual.<br>• Information will be protected using the procedures in Section 3.02. |
| Retention/ Destruction | • No redundant copies will be retained.<br>• PHI will be destroyed when no longer needed or 6 years after creation. |

### *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.<br>• Health care providers involved with treating the Participant<br>• Business Associates and Insurers involved in benefit determinations.<br>• 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.<br>• 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."<br>• Electronic records will be retained consistent with the Plan's HIPAA Security Manual.<br>• Information will be protected using the procedures in Section 3.02. |
| Retention/ Destruction | • No redundant copies will be retained.<br>• PHI will be destroyed when no longer needed or 6 years after creation. |

### 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.<br>• 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."<br>• Electronic records will be retained consistent with the Plan's HIPAA Security Manual.<br>• Information will be protected using the procedures in Section 3.02. |
| Retention/ Destruction | • No redundant copies will be retained.<br>• PHI will be destroyed when no longer needed or 6 years after creation. |

### d. Citations

45 CFR § 164.506

## 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

# 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<br>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).<br>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.

### 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.

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

# 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.

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.

### c. Citations

45 CFR § 164.514
45 CFR § 164.502(d)

# 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.

### 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

# 4.08 Protection of Privacy of Reproductive Health Care

## a. General Prohibition on Use or Disclosure

Each Plan and its Business Associates are prohibited from Using or Disclosing PHI for any of the following:

1. A criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating Reproductive Health Care
2. Imposing criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating Reproductive Health Care
3. Identifying any person for any purpose described in (1) or (2).

### Application of the General Prohibition

The prohibition described in this Section 4.08(a) applies when the Reproductive Health Care provided by someone other than the Plan or Business Association is presumed to be lawful. Reproductive Health Care provided by someone other than the Plan or Business Association is presumed to be lawful *unless*:

- The Plan or a Business Associate has actual knowledge that the Reproductive Health Care was not lawful under the circumstances in which it was provided or

- The Plan or a Business Associate receives factual information from the person making the PHI request that demonstrates a substantial factual basis that the Reproductive Health Care was not lawful under the circumstances in which it was provided.

The prohibition described in this Section 4.08(a) also applies if the Plan or a Business Associate that received the request for PHI has reasonably determined that the Reproductive Health Care:

- is lawful under the law of the state in which the health care is provided under the circumstances in which it is provided, or

- is protected, required, or authorized by Federal law, including the U.S. Constitution, regardless of the state in which the health care is provided.

A Plan or a Business Associate may Use or Disclose PHI for purposes otherwise permitted under the Privacy Rule and these Policies and Procedures.

## b. Attestation

If a request for PHI potentially related to Reproductive Health Care is for any of the following:

- Health oversight activities,
- Judicial and administrative proceedings,
- Law enforcement purposes, or
- Disclosures to coroners and medical examiners,

then the Privacy Official (or his or her designee) shall require the person making the request sign an attestation (Form located in Section 10.11).

To be valid, the attestation must be in a separate document and must include:

- The name of any individual(s) whose PHI is sought, if practicable. If not practicable, a description of the class of individuals whose PHI is sought
- The name or other specific identification of the person(s), or class of persons, who are requested to make the use or disclosure.
- The name or other specific identification of the person(s), or class of persons, to whom the covered entity is to make the requested use or disclosure.
- A clear statement that the use or disclosure is not for a prohibited purpose
- A statement that a person may be subject to criminal penalties pursuant to 42 U.S.C. 1320d-6 if that person knowingly and in violation of HIPAA obtains individually identifiable health information relating to an individual or discloses individually identifiable health information to another person.

Disclosure to law enforcement is only permitted when all three of the following are met:

- The disclosure is not subject to the prohibition;
- The disclosure is required by law (meaning that applicable law requires a response to the request for PHI); and
- The disclosure is in compliance with and is limited by:
  - A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer,

- A grand jury subpoena, or

- An administrative request, provided that the information sought is relevant and material to a legitimate law enforcement inquiry, the request is specific and limited in scope, and de-identified information could not reasonably be used. A new attestation is required for each specific use or disclosure request.

### c. Reproductive Health Care

Reproductive Health Care means health care that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes. This includes

- Contraception, including emergency contraception

- Preconception screening and counseling

- Management of pregnancy and pregnancy-related conditions, including pregnancy screening, prenatal care, miscarriage management, treatment for preeclampsia, hypertension during pregnancy, gestational diabetes, molar or ectopic pregnancy, and pregnancy termination

- Fertility and infertility diagnosis and treatment, including assisted reproductive technology (ART) such as in vitro fertilization (IVF)

- Diagnosis and treatment of conditions that affect the reproductive system (for example, perimenopause, menopause, endometriosis, adenomyosis)

- Other types of care, services, and supplies used for the diagnosis and treatment of conditions related to the reproductive system (for example, mammography, pregnancy-related nutrition services, postpartum care products).

### d. Processing a Request

Each Plan is responsible for receiving and processing requests for Use or Disclosure of PHI potentially related to Reproductive Health Care. Each Plan has assigned this responsibility to the Privacy Official. Requests must be sent to the Privacy Official (or his or her designee). Each Plan will develop procedures with its Business Associates to coordinate the responses to requests for Use of Disclosure of PHI potentially related to Reproductive Health Care in the Business Associates' custody.

#### Determinations

The Privacy Official (or his or her designee) shall determine if the prohibition described in

 

Section 4.08(a) applies to a request for Use or Disclosure of PHI potentially related to Reproductive Health Care.

In making this determination, the Privacy Official (or his or her designee) should presume the prohibition applies and may not rely solely on a statement of the person making the request that

- the Reproductive Health Care was unlawful under the circumstances in which it was provided, or
- that requested disclosure of PHI is not for a prohibited purpose.

However, the Privacy Official (or his or her designee) may take into account adequate supporting documentation provided by the person making the request.

The Privacy Official (or his or her designee) also shall determine if an attestation described in Section 4.08(b) is required. If an attestation, on its face, meets the requirements described in Section 4.08(b), the Privacy Official (or his or her designee) must consider the totality of the circumstances surrounding the attestation and whether it is reasonable to rely on the attestation in those circumstances. To determine whether it is reasonable to rely on the attestation, the Privacy Official (or his or her designee) should consider, among other things:

- who is requesting the Use or Disclosure of PHI,
- the permission upon which the person making the request is relying,
- the information provided to satisfy other conditions of the relevant permission,
- the PHI requested and its relationship to the purpose of the request (e.g., does the request meet the Minimum Necessary standard), and
- where the presumption described in Section 4.08(a), information provided by the person making the request to overcome that presumption.

The Privacy Official (or his or her designee) may generally rely on an attestation if, under the circumstances, he or she reasonably determines that the request is not for investigating or imposing liability for the mere act of seeking, obtaining, providing, or facilitating allegedly unlawful reproductive health care. In addition, the Privacy Official (or his or her designee) may generally rely on an attestation and any accompanying material if, under the circumstances, he or she reasonably could conclude that the requested disclosure of PHI is not for a prohibited purpose.

If the Privacy Official (or his or her designee) authorizes the Use or Disclosure or PHI related

to Reproductive Health Care, the Plan will limit the Use or Disclosure to the Minimum Necessary, unless one of the specified exceptions to the Minimum Necessary standard applies.

**Revocation of Prior Determination**

If, during the course of Using or Disclosing PHI potentially related to reproductive health care in reasonable reliance on a facially valid attestation, a Plan or Business Associate discovers information reasonably showing that any representation made in the attestation was materially false, leading to a Use or Disclosure for a prohibited purpose, the Plan or Business Associate must cease the Use or Disclosure.

### *e. Documenting Requests*

All requests for Use or Disclosure of PHI potentially related to Reproductive Health Care, attestations, and responses to those requests, including supporting statements, will be documented and retained for six years from the date the request was processed.

### *f. Citations*

45 C.F.R. § 164.502(a)(5)(iii)
45 C.F.R. § 164.509

# 5. Individual Rights

## 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.

# 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.

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.

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

six (6) years.

### h. Citations

45 CFR § 164.524

# 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

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

# 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

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)

# 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)

# 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.

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

# 6. Risk Management Activities

# 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.

# 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)

# 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.

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)

# 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)

# 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:

- 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.

### 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<br>✓ the incident was discovered when staff returned for regular working hours on August 2, 2010<br>✓ 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<br>✓ contact the free government *[free gov't service by website/address]*<br>✓ 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<br>✓ actively monitoring the progress of the police investigation<br>✓ will make all reasonable efforts to recover the missing computers<br>✓ 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

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

 

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

# 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)<br>☐ Authorizations<br>☐ Attestations<br>☐ Plan Amendments<br>☐ Plan Amendment certifications<br>☐ Business Associate Agreements<br>☐ Notices of Privacy Practices<br>☐ 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<br><br>☐ Name of contact person or office responsible for receiving complaints and providing additional privacy information<br><br>☐ 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<br><br>☐ 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 |

| 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)

# 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.

| Event | Recommended Action(s) |
|---|---|
| **Change in** VANDERBILT **Operations**:<br>• New staff members<br>• New technology<br>• New operating procedures | • Monitor and update any changes in HIPAA Privacy Complaint Manager (and other Contacts) listed in Section 10.03.<br>• Update and refer to Section 10.02 in the event of any change involving the Privacy Official.<br>• 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.<br>• Implement training appropriate to the level of any revisions in Policies and Procedures resulting from staffing, technology or operations changes.<br>• 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.<br>• Identify specific Policies and Procedures affected by the development.<br>• Assess need for modifications to the Policies and Procedures.<br>• Revise Policies and Procedures – including legal documents referenced in Section 7 and Participant forms referenced in Section 5 – as appropriate.<br>• Distribute revised Policies and Procedures and training materials.<br>• If applicable, distribute revised HIPAA Privacy Notice and Sponsor Certification.<br>• 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.<br>• Negotiate and customize the Business Associate agreement and present it for execution to the vendor.<br>• Amend Section 10.04b ("Log of Business Associate Agreements") and any other documents referring to the Business Associate.<br>• 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. |

| 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.<br>• 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.<br>• Amend Section 10.04b ("Log of Business Associate Agreements") and any other documents referring to the Business Associate.<br>• 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.<br>• Obtain and preserve contact information for purposes of referring future PHI requests.<br>• 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.<br>• Furnish Plan Sponsor Certification, as appropriate (if PHI will be obtained from the insurer).<br>• 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.<br>• Update and preserve contact information for purposes of referring requests for PHI maintained by insurer under a prior policy or contract.<br>• 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.) |

| 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).<br>• 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.<br>• Determine application of "organized health care arrangement" to all Plans, including modifications to Policies and Procedures and use of joint Notice of Privacy Practices.<br>• Amend Section 10.01 ("Covered Plans") and any other documents or forms referring to the Plans, as appropriate.<br>• Refer to guidelines above on "Business Associate Addition" or "Insurer Addition", as applicable.<br>• 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.<br>• 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.<br>• Amend Section 10.01 ("Covered Plans") and any other documents or forms referring to the Plans, as appropriate.<br>• Refer to guidelines above on "Business Associate Termination" or "Insurer Termination or Policy Revision" as applicable.<br>• Consider if changes in personnel also implicated.<br>• 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.<br>• 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.<br>• 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.<br>• Amend Section 10.01 ("Covered Plans") and any other documents or forms referring to the Plans, as appropriate.<br>• Refer to guidelines above on "Business Associate Addition" or "Insurer Addition" as applicable.<br>• Consider if changes in personnel are also implicated. |

| 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.<br>• Verify whether the subsidiary Plan is a separate group health plan or a component of another Plan.<br>• 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.<br>• Amend Section 10.01 ("Covered Plans") and any other documents or forms referring to the Plans, as appropriate.<br>• Refer to guidelines above on "Business Associate Termination" or "Insurer Termination or Policy Revision" as applicable.<br>• Consider if changes in personnel are also implicated. |

# 7. Required Legal Documents

# 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).

# 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.

### 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)

# 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)

# 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;<br>• Ensure that any vendors or agents to whom VANDERBILT provides PHI agree to the same restrictions;<br>• Not use or disclose the PHI for employment-related actions or in connection with any other benefit program of VANDERBILT;<br>• 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;<br>• Make PHI accessible to individuals in accordance with Section 4.02;<br>• Allow individuals to amend their information in accordance with Section 4.03;<br>• Provide an accounting of its disclosures in accordance with Section 4.06;<br>• Make its practices available to HHS for determining compliance;<br>• Return and destroy all PHI when no longer needed, if feasible; and<br>• 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.

### c. Citations

45 CFR § 164.504(f)(2)(ii)

# 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.

### 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)

# 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

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

# 7.07 Attestation

See Section 4.08 for further information.

### *a. Documentation Requirement*

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

### *b. Citations*

45 CFR § 164.509

# 8. Definitions

# 8.01 Definitions

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

***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

(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.

***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

 

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.

***Reproductive Health Care:*** Health Care that affects the health of an Individual in all matters related to the reproductive system and to its functions and processes. This definition will not be construed to set forth a standard of care for or regulate what constitutes clinically appropriate Reproductive Health Care.

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

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

# 9. HIPAA 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

# 10. Key Resources and Forms

10.01 Covered Plans

10.02 Privacy Official

10.03 Other Contacts

10.04 Business Associate Agreements

10.05 Insurers

10.06 Plan Sponsor Documentation

10.07 Notice of Privacy Practices

10.08 Participant Forms

10.09 Breach Report Forms

10.10 Legally Required Uses, Public Health Activities, Other Situations Not Requiring Authorization

10.11 Attestation

# 10.01 Covered Plans

Any self-insured medical, dental, vision, EAP, health FSA or long term care plan maintained by VANDERBILT.

# 10.02 Privacy Official

## *a. Privacy Official Designation*

The following person is designated as the Privacy Official:

| | |
|---|---|
| Name: | Julie Hanna |
| Address: | |
| Phone: | 615-343-6624 |
| Fax: | |
| Email: | Julie.Hanna@Vanderbilt.edu |
| Other contact information: | Benefits Operations Manager |
| | |

### b. Sample Privacy Official Job Description

The Privacy Official shall be responsible for coordinating employer's policies and procedures under HIPAA's privacy rules, as revised from time-to-time, monitoring compliance with those rules, and making decisions with respect to any issues that arise under such rules.

### c. Essential Duties – General

- *Serve as the leader of VANDERBILT's HIPAA privacy workgroup and focal point for privacy compliance-related activities*
- *Implement HIPAA privacy policies and procedures for VANDERBILT's group health plan arrangement*
- *Assist in the interpretation of the state and federal privacy rules and act as the designated decision-maker for issues and questions, in coordination with legal counsel*
- *Oversee training programs*
- *Ensure compliance with privacy practices and consistent application of sanctions for failure to comply within employer's workforce and all Business Associates, in cooperation with human resources, administration, and legal counsel as applicable*
- *Audit and administer privacy program reviews*
- *Serve as internal and external liaison and resource between the employer group health plan and other entities (employer's officers, vendors, Office of Civil Rights, other legal entities) for purposes of any compliance reviews or investigations and to ensure that employer's privacy practices are implemented, consistent, and coordinated*
- *Periodically revise the HIPAA privacy policies and procedures in light of changes to the rules, or changes in group health plan practices or in the flow of PHI*

### d. Essential Duties – Specific

- *Develop a procedure to inventory and document the uses and disclosures of protected health information (PHI)*
- *Assist in the development, implementation, negotiation, and compliance monitoring of Business Associate contracts to ensure all privacy concerns, requirements, and responsibilities are addressed*

- *Develop and implement overall privacy policies and procedures as applicable for the employer group health plan arrangement*

- *Develop and implement appropriate firewalls between employer functions and the functions of the group health plan arrangement*

- *Draft and distribute the HIPAA privacy notice*

- *Appoint or serve as the designated contact person in the privacy notice and receive questions and complaints related to the protection of PHI, participant privacy, and violations of employer's privacy procedures*

- *Establish mechanisms and monitor processes to ensure participants' rights to restrict, amend, have access to, and receive an accounting of their health information*

- *Establish and administer a process to receive, document, track, investigate, and take action (including developing sanctions) on all complaints regarding employer's privacy policies and procedures*

- *Ensure that employer develops and maintains appropriate privacy authorization forms*

- *Ensure that amendments to plan documents are addressed*

- *Ensure that all documentation required by the privacy rule is maintained and retained for six (6) years from the date it was created or was last in effect, whichever is later*

- *Oversee and ensure delivery of privacy training and orientation to staff*

- *Establish programs to audit and monitor Business Associates*

- *Monitor changes to the HIPAA privacy and security rules, including federal and state laws and regulations*

- *Establish programs to audit and monitor internal privacy compliance, perform initial and periodic privacy risk assessments, and conduct related ongoing compliance monitoring activities*

- *Review system-related information security plans as necessary throughout employer's network to ensure alignment between security and privacy practices, and act as a liaison to the information systems department*

The Privacy Official shall have the sole authority and discretion to delegate the above tasks or portions thereof to other individuals within employer or to consultants, contractors or other specialists, as appropriate, provided that the Privacy Official monitors such activities in good faith for purposes of achieving compliance with HIPAA.

# 10.03 Other Contacts

The following is a list of key contacts (persons or offices) responsible for responding to Participants exercising their rights described in Section 5; for receiving complaints concerning 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.

- Inspection Contact

| | |
|---|---|
| Name: | Privacy Official |
| Address: | |
| Phone: | |
| Fax: | |
| E-mail: | |

- Amendment Contact

| | |
|---|---|
| Name: | Privacy Official |
| Address: | |
| Phone: | |
| Fax: | |
| E-mail: | |

- Restriction Contact

| | |
|---|---|
| Name: | Privacy Official |
| Address: | |
| Phone: | |
| Fax: | |
| E-mail: | |

- Communications Contact

| | |
|---|---|
| Name: | Privacy Official |
| Address: | |
| Phone: | |
| Fax: | |
| E-mail: | |

- Disclosure Contact

| | |
|---|---|
| Name: | Privacy Official |
| Address: | |
| Phone: | |
| Fax: | |
| E-mail: | |

- Complaint Manager

| | |
|---|---|
| Name: | Privacy Official |
| Address: | |
| Phone: | |
| Fax: | |
| E-mail: | |

- Authorization Contact

| | |
|---|---|
| Name: | Privacy Official |
| Address: | |
| Phone: | |
| Fax: | |
| E-mail: | |

- Breach Contact

| | |
|---|---|
| Name: | Privacy Official |
| Address: | |
| Phone: | |
| Fax: | |
| E-mail: | |

# 10.04 Business Associate Agreements

## *a. Model Business Associate Agreement*

| Directions to VANDERBILT for Using Model Business Associate Agreement |
|---|
| **General Comments**. This model consolidated Privacy and Security HIPAA Business Associate Agreement is designed to be an addendum to an existing contract between VANDERBILT and its third party vendor. It should be modified if it will be used as a stand-alone contract (i.e., there is no existing contract), or for insertion into the body of a contract. This model is drafted with the intent that the Business Associate is an independent contractor. Employers may be liable for the acts and omissions of their Business Associates that violate HIPAA Privacy and Security requirements if the Business Associates are acting as their agents (rather than independent contractors) and the violations are within the scope of their agency. Whether an agency relationship exists depends on all the facts and circumstances (for further information see 78 Fed. Reg. 5580-5582, Jan. 25, 2013).<br><br>Note that regulatory updates published in 89 Fed. Reg. 32976, have required updates to the model Business Associate Agreement, effective December 23, 2024. A general statement of compliance with these rules is included in this model agreement.<br><br>**Select Instructions:**<br>**Section 3.0(b).** This section is optional. Most vendors will likely request the authority to engage in the specific uses and disclosures discussed therein.<br>**Section 4.0(a) and (b).** VANDERBILT will need to modify this subsection if it delegated to the Business Associate its obligation to produce and provide Privacy Notices.<br>**Section 6.0(a).** The Term of the Agreement is subject to negotiation by the parties. For the Agreement's effective date, VANDERBILT would typically propose the beginning date (or last renewal date) of the contract.<br>**Section 7.0(g).** Conform this section to the existing contract with this vendor unless that contract does not specify the law of which state will govern the contract.<br>**Section 7.0(h)**. Modify this section if the existing contract does not include any provision regarding indemnification or performance guarantees, if application of those provisions requires additional statements in this section, and/or if the proposed sample text is inappropriate to the parties. |

**HIPAA PRIVACY AND SECURITY BUSINESS ASSOCIATE AGREEMENT**
**(AS OF 05/31/13)**

This Agreement is entered into this _____ day of _____, _____, between [*Employer*] ("Employer"), acting on behalf of [*Name of covered entity/plan(s) for which vendor provides services*] (the "Plan(s)"), and [*Name of vendor*] ("Business Associate"). The Agreement is incorporated into the [*Name of vendor contract*] between Employer and Business Associate, dated [*Date of Contract*] (the "Contract"). The parties intend to use this Agreement to satisfy the Business Associate contract requirements in the regulations at 45 CFR §§ 164.502(e), 164.504(e) and 164.314(a), issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5) and regulations promulgated thereunder; and for further applicable HIPAA developments published after enactment of P.L. 111-5, including statutes, case law, regulations and other agency guidance. Specifically, the parties intend to use this Agreement to satisfy applicable requirements effective beginning December 23, 2024, under regulations published in 89 Fed. Reg. 32976. [*If there is no existing applicable vendor agreement, then this agreement will be a letter agreement between employer and the vendor*.]

### 1.0 Definitions

Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms in 45 CFR part 160 and part 164, including sections 160.103, 164.103, 164.304 and 164.501. Notwithstanding the above, "Covered Entity" shall mean the [*Name of covered entity/plan*]; "Individual" shall mean the person who is the subject of the Protected Health Information and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g); Protected Health Information shall have the meaning defined in 45 CFR § 160.103, which also sets forth the definition of health information, including genetic information as clarified by P.L. 110-233 and applicable regulations; "Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or his designee; "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E; and "Security Rule" shall mean the Standards for Security of Electronic Protected Health Information at 45 CFR part 160 and part 164, subparts A and C.

### 2.0 Obligations and activities of Business Associate

Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by Section 3.0 of this Agreement, or as required by law.

(a) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

(b) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

(c) Business Associate agrees to report to Covered Entity, in writing, any use or disclosure of the Protected Health Information not provided for by this Agreement and any security incident of which it becomes aware. [For purposes of this Agreement, "security incident" shall mean successful unauthorized access to, use, disclosure, modification or destruction of, or interference with, the electronic Protected Health Information.] *or* ["security incident" shall have the same meaning as the term "security incident" in 45 CFR § 164.304.] [*If the client prefers to narrow the meaning of security incident to only include successful unauthorized access of e-PHI, use the first bracketed text above and (d) below. Otherwise, the agreement can use the second bracketed text cross referencing the regulation.*]

(d) [Upon request from Covered Entity, Business Associate agrees to provide information to Covered Entity on unsuccessful unauthorized access, use, disclosure, modification or destruction of the electronic Protected Health Information to the extent such information is available to Business Associate.] [*Use this text only if the definition of security incident is narrowed by using the text in the first bracket in (c) above.*]

(e) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information or electronic Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity agrees, in writing, to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

(f) Business Associate agrees to provide access, at the request of Covered Entity or an Individual, and in a prompt and reasonable manner consistent with the HIPAA regulations to Protected Health Information in a designated record set, to the Covered Entity or directly to an Individual in order to meet the requirements under 45 CFR § 164.524.

(g) Business Associate agrees to make any amendment(s) to Protected Health Information in a designated record set that the Covered Entity or an Individual directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual, and in a prompt and reasonable manner consistent with the HIPAA regulations.

(h) Business Associate agrees to make its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or at the request of the Covered Entity, to the Secretary in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

(i) Business Associate agrees to document disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

(j) Business Associate agrees to provide to Covered Entity or an Individual an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528, in a prompt and reasonable manner consistent with the HIPAA regulations [*but in no event later than thirty (30) days after receiving a request for such an accounting*].

(k) Business Associate agrees to satisfy all applicable provisions of HIPAA standards for electronic transactions and code sets, also known as the Electronic Data Interchange (EDI) Standards, at 45 CFR Part 162, as well as all operating rules that apply to standard transactions, submission of certifications to HHS (to the extent HHS permits) concerning standard transactions, and all other electronic data interchange requirements included in the Patient Protection and Affordable Care Act of 2010. Business Associate further agrees to ensure that any agent, including a subcontractor, that conducts standard transactions on its behalf will comply with the EDI Standards.

(l) Business Associate agrees to determine the minimum necessary type and amount of PHI required to perform its services and will comply with 45 CFR § 164.502(b) and 514(d).

(m) Business Associate agrees to restrict the use or disclosure of Protected Health Information as may be agreed to in accordance with 45 CFR § 164.522, to document those restrictions, and to provide to Covered Entity such documentation, upon request, and in a prompt and reasonable manner consistent with the HIPAA regulations.

(n) Business Associate agrees to accommodate alternative means or alternative locations to communicate Protected Health Information, and document those alternative means or alternative locations, at the request of Covered Entity or an Individual, pursuant to 45 CFR § 164.522(b), in a prompt and reasonable manner consistent with the HIPAA regulations.

(o) Business Associate agrees to be the primary party responsible for receiving and resolving requests from an Individual exercising his or her individual rights described in subsections (f), (g), (j), and (n) of this section 2.0.

(p) Business Associate agrees to implement any and all administrative, technical and physical safeguards necessary to reasonably and appropriately protect the confidentiality, integrity and availability of electronic Protected Health Information that it creates, receives,

maintains or transmits on behalf of the Plan(s), including ensuring compliance with 45 CFR §§ 164.308, 164.310, 164.312, 164.314 and 164.316.

(q) Business Associate agrees to ensure that access to electronic Protected Health Information related to the Covered Entity is limited to those workforce members who require such access because of their role or function.

(r) Business Associate agrees to implement safeguards to prevent its workforce members who are not authorized to have access to such electronic Protected Health Information from obtaining access and to otherwise ensure compliance by its workforce with the Security Rule.

(s) Business Associate shall, following the discovery of a breach of unsecured Protected Health Information, as defined by 45 CFR § 164.402, notify Covered Entity of such breach in a manner compliant with the terms of 45 CFR § 164.410. Business Associate shall be responsible for notification of Individuals and any governmental entities requiring notification. Such notification will contain the elements required in 45 CFR § 164.410 or applicable state law. [*Business Associate agrees that Covered Entity will be given reasonable advance opportunity to review the proposed notice or other related communications to any individual or third party regarding the breach; Covered Entity may propose revised or additional content to the materials which will be given reasonable consideration by Business Associate (or its agent).*]

(t) [*Business Associate shall not receive direct or indirect remuneration for any exchange of Protected Health Information otherwise authorized under the Privacy and/or Security Rules without an Individual's authorization.*]

(u) Business Associate acknowledges that enactment of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5, ARRA) amended certain provisions of HIPAA in ways that now directly regulate Business Associate's obligations and activities under HIPAA's Privacy Rule and Security Rule including the Breach Notification Rule. Business Associate agrees to comply, as of the applicable effective dates of each such HIPAA obligation relevant to Business Associate, with the requirements imposed by ARRA, including monitoring federal guidance and regulations published thereunder and timely compliance with such guidance and regulations. In consequence of the foregoing direct regulation of Business Associate by HIPAA laws and regulations, notwithstanding any other provision of the Agreement, Business Associate further agrees to monitor HIPAA Privacy and Security requirements imposed by future laws and regulations, and to timely comply with such requirements when acting for or on behalf of the Plan in its capacity as a Business Associate.

**3.0 Permitted or required uses and disclosures by Business Associate**

(a) **General use and disclosure.**

(i) Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Contract and in this Agreement, provided that such use or disclosure of Protected Health Information would not violate the Privacy Rule, including the minimum necessary requirement, if done by Covered Entity.

(ii) Business Associate shall share Protected Health Information as reasonably requested by Covered Entity (and as permitted by Section 5.0) with Covered Entity and the Centers for Medicare and Medicaid Services (CMS), and with their agents and any other parties permitted by CMS guidance (including CMS' FAQ #5482), where the Covered Entity is submitting to CMS the Protected Health Information required by 42 CFR 423.884 for Medicare's retiree drug subsidy program.

(iii) [*If not specified in the contract, consider adding provisions clearly obligating business associate to share protected health information for permitted purposes, such as for audits performed by business associates or employer. For example:* "Business Associate shall share Protected Health Information as reasonably requested by Employer (and as permitted by Section 5.0) to carry out its responsibilities as plan administrator of the Plan(s), including, without limitation, for purposes of auditing the performance of Business Associate."]

(b) **Additional use and disclosure.**

(i) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(ii) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that such disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the

person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(iii) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide data aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B).

(iv) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR § 164.502(j)(1).

(c) **Reproductive Health Care use and disclosure**

(i) Business Associate agrees to prohibit the use and disclosure of Protected Health Information for any reason specified in 45 CFR § 164.502(a)(5)(iii), which generally relates to criminal, civil, or administrative investigations or impositions of liability (including the identification of any person for such purposes) relating to any person for the mere act of seeking, obtaining, providing, or facilitating Reproductive Health Care. [*Optional: Business Associate additionally agrees to notify Covered Entity of any request related to Reproductive Health Care.*] Furthermore, Business Associate agrees to require a valid attestation (in compliance with the requirements outlined in 45 CFR § 164.509(b)(1)), a copy of which shall be made available to Covered Entity upon request, before using or disclosing Protected Health Information potentially related to Reproductive Health Care for any of the following purposes: health oversight activities, judicial and administrative proceedings, law enforcement purposes, or disclosures to coroners and medical examiners. Furthermore, Business Associate will cease use and disclosure and notify Covered Entity as soon as possible (but in no event in more than 3 days) after it acquires actual knowledge that material information in the attestation is false, or discovers information reasonably showing that any representation made in the attestation was materially false, leading to a use or disclosure prohibited by 45 CFR § 164.502(a)(5)(iii).

**4.0 Obligation to inform Business Associate of Covered Entity's privacy practices and any authorization or restriction**

(a) Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR § 164.520, as well as any changes to such notice.

(b) Covered Entity shall provide Business Associate with any changes in, or revocation of, authorization by Individual or his or her personal representative to use or disclose Protected Health Information, if such changes affect Business Associate's uses or disclosures of Protected Health Information.

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR § 164.522, if such changes affect Business Associate's uses or disclosures of Protected Health Information.

### 5.0 Permissible requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

### 6.0 Term and termination

(a) **Term.** The term of this Agreement shall be effective as of _____**,** and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

**(b) Termination for cause.** Without limiting the termination rights of the parties pursuant to the Contract, and upon Covered Entity's knowledge of a material breach by Business Associate of a provision under this Agreement, Covered Entity may, in its sole discretion, terminate the Agreement, with or without advance notice, and with or without an opportunity to cure the breach. [Alternatively, the Covered Entity may, in its sole discretion, provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Contract if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, or immediately terminate the Contract if Business Associate has breached a material term of this Agreement and cure is not possible. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.] [*Use bracketed text if client is willing to offer the vendor a right to cure a material breach.*]

(c) **Effect of termination.** The parties mutually agree that it is essential for Protected Health Information to be maintained after the expiration of the Agreement for regulatory and other business reasons. The parties further agree that it would be infeasible for Covered Entity to maintain such records because Covered Entity lacks the necessary system and expertise. Accordingly, Covered Entity hereby appoints Business Associate as its custodian for the safe keeping of any record containing Protected Health Information that Business Associate may determine it is appropriate to retain. Notwithstanding the expiration or termination of the Contract, Business Associate shall extend the protections of this Agreement to such Protected Health Information, and limit further use or disclosure of the Protected Health Information to those purposes that make the return or destruction of the Protected Health Information infeasible.

### 7.0 Miscellaneous

(a) **Regulatory references.** A reference in this Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended, and for which compliance is required.

(b) **Amendment.** Upon the enactment of any law or regulation affecting the use, disclosure, or safeguarding of Protected Health Information or electronic Protected Health Information, or the publication of any decision of a court of the United States or any state relating to any such law or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, either party may, by written notice to the other party, amend the Contract and this Agreement in such manner as such party determines necessary to comply with such law or regulation. If the other party disagrees with such amendment, it shall so notify the first party in writing within thirty (30) days of the notice. If the parties are unable to agree on an amendment within thirty (30) days thereafter, then either of the parties may terminate the Contract on thirty (30) days written notice to the other party. [*May be modified to fit parties' wishes*.]

(c) **Survival.** The respective rights and obligations of Business Associate under Section 6.0 of this Agreement shall survive the termination of this Agreement.

(d) **Interpretation.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy and Security Rules.

(e) **No third party beneficiary.** Nothing expressed or implied in this Agreement or in the Contract is intended to confer, nor shall anything herein confer, upon any person other than the parties and the respective successors or assignees of the parties, any rights, remedies, obligations, or liabilities whatsoever.

(f) **Severability.** If any provision of this Agreement is held illegal, invalid, prohibited or unenforceable by a court of competent jurisdiction, that provision shall be limited or eliminated in that jurisdiction to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect and enforceable.

(g) **Governing law.** This Agreement shall be governed by and construed in accordance with the laws of the state of _____ to the extent not preempted by the Privacy or Security Rules or other applicable federal law.

(h) **Agency.** The parties agree that Business Associate is not and will not act as an agent of Covered Entity. [*Optional text: Business Associate will indemnify Employer and/or Covered Entity for any and all losses and expenses, including but not limited to reasonable attorneys' fees, relating to claims that Business Associate has acted as Covered Entity's or Employer's agent.*]

(i) **Indemnification and performance guarantees.** The indemnification and performance guarantee provisions contained in the Contract shall also apply to this Agreement. *[Optional text: Further, notwithstanding any other provision of the Agreement or underlying services contract(s) between the parties, Business Associate agrees to pay all penalties and reasonable expenses, including those incurred for reasonable remediation, as a result of Business Associate's (or its agent's) acts or omissions related to its HIPAA obligations or through contractual agreement between the Business Associate and Plan.]*

| | |
|---|---|
| [*For Employer*] | [*For Vendor*] |
| By: _____ | By: _____ |
| Name: _____ | Name: _____ |
| Title: _____ | Title: _____ |
| Date: _____ | Date: _____ |

## *b. Log of Business Associate Agreements*

| Vendor Name | Agreement Date |
|---|---|
| | |

## 10.05 Insurers

The Plan may have components that are insured through Insurers. The names of such Insurers are available by contacting the Privacy Official.

# 10.06 Plan Sponsor Documentation

## *a. Amendment to Existing Plan Documents*

| Instructions for Completing Plan Amendment |
|---|
| **General & Introductory Paragraphs.** In order to receive PHI from a HIPAA covered plan, VANDERBILT will need to amend the Plan Document to comply with HIPAA's Privacy requirements and certify to the Plan that the appropriate Amendments have been made. The process for amending each plan will usually be described in the document creating the Plan. Amendment may require approval by a Board of Directors, Board of Trustees or another person specified by the Plan's Amendment provision. |
| The sample Amendment assumes there is a separate Plan Document for each covered plan. It is a "master Amendment" intended to amend all of VANDERBILT's Plan Documents. Alternatively, the "master Amendment" may be tailored for a single plan (or a group of fewer than all of VANDERBILT's plans). From the list of covered plans in Section 10.01, only the names of the plans from which the Plan Sponsor receives PHI need be listed in the introductory paragraph of the Amendment.<br>**[Bracketed text]** —Bracketed text is used to indicate where information should be specific to VANDERBILT. |

| Selected Line Instructions |
|---|
| **1.** If VANDERBILT sponsors one (1) or more small group health plans in addition to other covered plans, a separate Amendment might be appropriate as an alternative to stating a separate effective date for the small plan Amendment. |
| **2.a. & b.** Refer to Section 4.03 to determine the extent to which VANDERBILT's Plan administrative activities should be described. (Note that changes to these provisions should be reflected in the Notice of Privacy Practices.) |
| **5.i.(1)** Refer to Section 4.03 for a description of persons that may have access to PHI. This description may need to distinguish among various plans if the persons with access to PHI vary by plan. |
| **5.i.(3)** Coordinate disciplinary measures with those in Section 6.04 . |

 

**HIPAA PRIVACY AND SECURITY**
**MASTER GROUP HEALTH PLAN AMENDMENT**
**FOR GROUP HEALTH PLANS OF**
VANDERBILT

WHEREAS, under privacy and security rules of the Health Insurance Portability and Accountability Act of 1996, ("HIPAA"), and the regulations issued thereunder at 45 CFR Parts 160 and 164 ("the HIPAA regulations"), a group health plan must : (i) restrict the use and disclosure of protected health information ("PHI"), (ii) ensure the confidentiality, integrity, and availability of all electronic protected health information ("e-PHI") the plan creates, receives, maintains, or transmits, (iii) protect against any reasonably anticipated threats or hazards to the security and integrity of such information, (iv) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA privacy rules set forth in 45 CFR Part 164, Subpart E, and (v) ensure compliance with the HIPAA security rules set forth in 45 CFR Part 164, Subpart C by its workforce;

WHEREAS, [*Employer*] sponsors and maintains the following group health plans that are subject to the HIPAA regulations: [*list names of group health plans from Privacy Manual Section 10.01, or as otherwise determined*];

WHEREAS, [*Employer*] and/or agents representing [*Employer*] intend to receive PHI (some of which may be e-PHI) from the Plan (including its Business Associates, health insurance issuers, HMOs, and their agents) from time to time;

WHEREAS, the HIPAA regulations require [*Employer*] to amend the Plan to incorporate provisions specified in 45 CFR §§ 164.504(f)(2) & 164.314(b)(2) prior to the receipt of PHI and e-PHI; and

WHEREAS, [*name of person or entity having authority to amend plans for HIPAA privacy and security*] is authorized under [*identify section of plans or other basis establishing authority to amend plans*] to approve Amendments to the Plans;

NOW, THEREFORE, each respective Plan is hereby amended, as set forth below, to implement appropriate protections required under the HIPAA regulations.

1. **Effective date**. This Amendment is effective as of *[insert date].*

2. **Uses and disclosures of PHI.** The Plan and [*Employer*] may disclose a Plan Participant's PHI to [*Employer*] (or to [*Employer*]'s agent) for the following Plan administration functions under 45 CFR § 164.504(a), to the extent not inconsistent with the HIPAA regulations: [*insert activities set forth in Privacy Manual Section 4.03, or as otherwise determined*.]

3**. Restriction on Plan disclosure to [*Employer*].** Neither the Plan nor any of its Business Associates, health insurance issuers, or HMOs, will disclose PHI to [*Employer*] except upon the Plan's receipt of [*Employer*] certification that the Plan has been amended to incorporate the agreements of [*Employer*] under paragraph 4, except as otherwise permitted or required by law.

4**. Privacy agreements of [*Employer*].** As a condition for obtaining PHI from the Plan, its Business Associates, Insurers, and HMOs, [*Employer*] agrees it will:

a. not use or further disclose such PHI other than as permitted by paragraph 2 of this Amendment, as permitted by 45 CFR § 164.508, 45 CFR § 164.512, and, where applicable, 45 CFR 164.509, and other sections of the HIPAA regulations, or as required by law;

b. ensure that any of its vendors or agents to whom it provides the PHI agree to the same restrictions and conditions that apply to [*Employer*] with respect to such information;

c. not use or disclose the PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of [*Employer*];

d. report to the Plan any use or disclosure of the PHI that is inconsistent with the uses or disclosures provided for of which [*Employer*] becomes aware including reporting any breach of unsecured PHI;

e. make the PHI of a particular Participant available for purposes of the Participant's requests for inspection, copying, and Amendment, and carry out such requests in accordance with HIPAA regulation 45 CFR §§ 164.524 and 164.526;

f. make the PHI of a particular Participant available for purposes of required accounting of disclosures by [*Employer*] pursuant to the Participant's request for such an accounting in accordance with HIPAA regulation 45 CFR § 164.528;

g. make [*Employer*]'s internal practices, books, and records relating to the use and disclosure of PHI received from the Plan available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining compliance by the Plan with HIPAA;

h. if feasible, return or destroy all PHI received from the Plan that [*Employer*] still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, [*Employer*] agrees to limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

i. ensure that there is adequate separation between the Plan and [*Employer*] by implementing the terms of subparagraphs (1) through (3), below:

(1) **Employees with access to PHI.** The following employees or other individuals under the control of [*Employer*] are the only individuals that may access PHI received from the Plan: [*insert designations by name, position, title, department, or other classification; be sure to cover all persons providing plan administration functions*].

(2) **Use limited to Plan Administration.** The access to and use of PHI by the individuals described in (1), above, is limited to Plan Administration functions as defined in HIPAA regulation 45 CFR § 164.504(a) that are performed by [*Employer*] for the Plan.

(3) **Mechanism for resolving noncompliance.** If [*Employer*] or any other person(s) responsible for monitoring compliance determines that any person described in (1), above, has violated any of the restrictions of this Amendment, then such individual shall be disciplined in accordance with the policies of [*Employer*] established for purposes of privacy compliance, up to and including dismissal from employment. [*Employer*] shall arrange to maintain records of such violations along with the persons involved, as well as disciplinary and corrective measures taken with respect to each incident.

5. **Security agreements of [*Employer*].** As a condition for obtaining e-PHI from the Plan, its Business Associates, Insurers, and HMOs, [*Employer*] agrees it will:

a. implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the Plan;

b. ensure that the adequate separation between the Plan and [*Employer*] as set forth in 45 CFR § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;

c. ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information;

d. report to the Plan any Security Incident of which it becomes aware. For purposes of this Amendment, "Security Incident" shall mean successful unauthorized access to, use, disclosure, modification or destruction of, or interference with, the e-PHI; and

e. upon request from the Plan, [*Employer*] agrees to provide information to the Plan on unsuccessful unauthorized access, use, disclosure, modification or destruction of the e-PHI to the extent such information is available to [*Employer*].

6. **PHI not subject to this Amendment**. Notwithstanding the foregoing, the terms of this Amendment [*other than paragraph 5*] shall not apply to uses or disclosures of Enrollment, Disenrollment, and Summary Health Information made pursuant to 45 CFR § 164.504 (f)(l)(ii) or (iii); of PHI released pursuant to an Authorization that complies with 45 CFR § 164.508; or in other circumstances as permitted by the HIPAA regulations. [*Use bracketed reference to paragraph 5 if and only if: (a) e-PHI beyond enrollment, disenrollment, summary health information, and authorized disclosures is obtained by employer, AND (b) employer adopts literal interpretation of 164.314(b)(1), which would apply paragraph 5 unless the ONLY e-PHI obtained is enrollment, disenrollment, summary health information, or authorized disclosures.*]

7. **Definitions.** All capitalized terms within this Amendment not otherwise defined by the provisions of this Amendment shall have the meaning given them in the respective Plan or, if no other meaning is provided in the Plan, the term shall have the meaning provided under HIPAA.

8. **Copies effective as originals.** A copy of the signed and dated original of this Amendment shall be as effective as the original, and either an original or such copy shall be appended to the governing instruments of each Plan and shall be deemed to be a part of such governing instruments.

IN WITNESS WHEREOF, this Amendment was executed by the following duly authorized individual on behalf of [*identify entity having amending authority*] this ___ day of _____, 20 _.

VANDERBILT: _____ Date: _____

Print name: _____ Title: _____

### *b. Certification*

| Instructions for Completing Plan Sponsor Certification |
| --- |
| **General.** Two (2) sample certifications are included below. VANDERBILT may choose to describe the pertinent provisions of the Plan Amendment in its certification. The first sample certificate (the "Summary Form") takes this approach. The Summary Form includes the elements generally required by the HIPAA regulations, but it does not include the Amendment verbatim. (This form designates a single plan in the introductory paragraph, but it may be modified to cover more than one (1) plan.) Alternatively, VANDERBILT may choose to provide a brief certificate (the "Alternative Form") that references VANDERBILT's detailed HIPAA Privacy Amendment. |
| One advantage to the Summary Form is that if VANDERBILT changes its privacy amendment, the certification may not need to be revised (unless the change affects the certificate's description).<br>Certain vendors will require a complete copy of the HIPAA Privacy Amendment. If so, the "Alternative Form" (the second form provided below) may be the more appropriate form to use because attached will be a copy of the complete HIPAA Privacy Plan Amendment, as adopted. If VANDERBILT uses the Alternative Form, it should consider whether any provisions of the Amendment are inappropriate to furnish to the particular vendor.<br>**[Bracketed text]** — Each form of certificate contains bracketed text indicating where information should be specific to VANDERBILT. |

**PLAN SPONSOR CERTIFICATION OF**
**HIPAA PRIVACY PLAN AMENDMENTS**
**FOR** VANDERBILT
**[GROUP HEALTH PLAN]**

The undersigned duly authorized representative of VANDERBILT, Plan Sponsor of the **[Group Health Plan]** (the "Plan"), certifies by this instrument that the governing Plan was amended, effective **[date HIPAA Privacy Amendment was effective for Plan]**, to incorporate the provisions described below:

**Privacy Agreements of** VANDERBILT. As a condition for obtaining PHI from the Plan (including PHI from any Business Associate, health insurance issuer or HMO), VANDERBILT agrees it will:

a. Not use or further disclose such PHI other than as permitted by the terms of the Plan or governing law;

b. Ensure that any of its agents or vendors to whom it provides the PHI agree to the same restrictions and conditions that apply to VANDERBILT with respect to such information;

c. Not use or disclose the PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of VANDERBILT;

d. Report to the Plan any use or disclosure of the PHI that is inconsistent with the uses or disclosures provided for of which VANDERBILT becomes aware including reporting to the Plan any breaches of unsecured PHI;

e. Make the PHI of a particular Participant available for purposes of the Participant's requests for inspection, copying, and Amendment, and carry out such requests in accordance with HIPAA 45 CFR §§ 164.524 and 164.526;

f. Make the PHI of a particular Participant available for purposes of an accounting required of any disclosures by VANDERBILT pursuant to the Participant's request for such an accounting in accordance with HIPAA 45 CFR § 164.528;

g. Make VANDERBILT's internal practices, books, and records relating to the use and disclosure of PHI received from the Plan available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining compliance by the Plan with HIPAA;

h. If feasible, return or destroy all PHI received from the Plan that VANDERBILT still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, VANDERBILT agrees to limit further uses and disclosures to those purposes that

make the return or destruction of the information infeasible; and

i. Ensure that there is adequate separation between the Plan and VANDERBILT by implementing provisions of the Plan describing persons or classes of persons employed or controlled by VANDERBILT who may access Plan PHI, restricting the access and use of PHI by those persons to Plan Administrative functions, and providing a mechanism for resolving issues caused by such persons' noncompliance with the Plan's provisions regarding use and disclosure of PHI.

This certification is provided in accordance with the regulations issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

Being duly authorized by VANDERBILT, the undersigned hereby certifies by execution of this instrument on this ____ day of _____, _____, that the **[Group Health Plan]** was amended to include the provisions described above, and that VANDERBILT agrees to such provisions.

VANDERBILT

By: _____

_____
*(print name)*

Title: _____

## ALTERNATIVE FORM OF PLAN SPONSOR CERTIFICATION

**PLAN SPONSOR CERTIFICATION OF**
**HIPAA PRIVACY PLAN AMENDMENTS FOR**
VANDERBILT
**[GROUP HEALTH PLAN]**

The undersigned duly authorized representative of VANDERBILT, Plan Sponsor of the **[Group Health Plan]** (the "Plan"), certifies by this instrument that the Plan was amended, effective **[date HIPAA Privacy Amendment was effective for Plan],** by adoption of the "HIPAA Privacy Master Group Health Plan Amendment for Group Health Plans of VANDERBILT" attached to this certificate. The undersigned further certifies that VANDERBILT agrees to the provisions in such Amendment.

VANDERBILT

By: _____

_____
*(print name)*

Date: _____

Title: _____

*(Attach amendment)*

# 10.07 Notice of Privacy Practices

| Instructions for Privacy Notice |
| --- |
| This sample was designed as a joint Privacy Notice for all group health plan self-insured benefits. If appropriate, indicate which components of the plans are covered by this notice (self-funded? insured? which options?). Employers may choose to send multiple notices for different benefits, in which case the notices should be modified accordingly.<br>Note that if a use or disclosure is prohibited or materially limited by another law — e.g., a more stringent state law — the notice must reflect the more stringent requirements (45 CFR § 164.520(b)(1)(ii)).<br>The notice must describe how the individual may exercise each individual right and should indicate where to submit requests (e.g., Plan Contact, Insurer, Business Associate?). |

# SAMPLE PRIVACY NOTICE

## Please carefully review this notice. It describes how medical information about you may be used and disclosed and how you can get access to this information.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) imposes numerous requirements on the use and disclosure of individual health information by VANDERBILT health plans. This information, known as protected health information, includes almost all individually identifiable health information held by a plan – whether received in writing, in an electronic medium, or as an oral communication. This notice describes the privacy practices of these plans: [*list plans covered under joint notice*]. The plans covered by this notice may share health information with each other to carry out treatment, payment, or health care operations. These plans are collectively referred to as the Plan in this notice, unless specified otherwise.

### The Plan's duties with respect to health information about you

The Plan is required by law to maintain the privacy of your health information and to provide you with this notice of the Plan's legal duties and privacy practices with respect to your health information. If you participate in an insured plan option, you will receive a notice directly from the Insurer. It's important to note that these rules apply to the Plan, not *[VANDERBILT]* as an employer – that's the way the HIPAA rules work. Different policies may apply to other [VANDERBILT] programs or to data unrelated to the Plan.

### How the Plan may use or disclose your health information

The privacy rules generally allow the use and disclosure of your health information without your permission (known as an authorization) for purposes of health care treatment, payment activities, and health care operations. Here are some examples of what that might entail:

- ***Treatment*** includes providing, coordinating, or managing health care by one or more health care providers or doctors. Treatment can also include coordination or management of care between a provider and a third party, and consultation and referrals between providers. *For example, the Plan may share your health information with physicians who are treating you.*

- **Payment** includes activities by this Plan, other plans, or providers to obtain premiums, make coverage determinations, and provide reimbursement for health care. This can include eligibility determinations, reviewing services for medical necessity or appropriateness, utilization management activities, claims management, and billing; as well as "behind the scenes" plan functions such as risk adjustment, collection, or reinsurance. *For example, the Plan may share information about your*

*coverage or the expenses you have incurred with another health plan in order to coordinate payment of benefits.*

- **Health care operations** include activities by this Plan (and in limited circumstances other plans or providers) such as wellness and risk assessment programs, quality assessment and improvement activities, customer service, and internal grievance resolution. Health care operations also include vendor evaluations, credentialing, training, accreditation activities, underwriting, premium rating, arranging for medical review and audit activities, and business planning and development. *For example, the Plan may use information about your claims to audit the third parties that approve payment for Plan benefits.*

The amount of health information used, disclosed or requested will be limited and, when needed, restricted to the minimum necessary to accomplish the intended purposes, as defined under the HIPAA rules. If the Plan uses or discloses PHI for underwriting purposes, the Plan will not use or disclose PHI that is your genetic information for such purposes.

**How the Plan may share your health information with** VANDERBILT

The Plan, or its health insurer or HMO, may disclose your health information without your written authorization to [VANDERBILT] for plan administration purposes. [VANDERBILT] may need your health information to administer benefits under the Plan. [VANDERBILT] agrees not to use or disclose your health information other than as permitted or required by the Plan documents and by law. [*identify classes of employees, e.g., benefits staff, payroll, finance*] are the only [VANDERBILT] employees who will have access to your health information for plan administration functions.

Here's how additional information may be shared between the Plan and [VANDERBILT], as allowed under the HIPAA rules:

- The Plan, or its insurer or HMO, may disclose "summary health information" to [VANDERBILT] if requested, for purposes of obtaining premium bids to provide coverage under the Plan, or for modifying, amending, or terminating the Plan. Summary health information is information that summarizes participants' claims information, from which names and other identifying information have been removed.

- The Plan, or its insurer or HMO, may disclose to [VANDERBILT] information on whether an individual is participating in the Plan or has enrolled or disenrolled in an insurance option or HMO offered by the Plan.

In addition, you should know that [VANDERBILT] cannot and will not use health information obtained from the Plan for any employment-related actions. However, health information collected by [VANDERBILT] from other sources, for example under the Family and Medical Leave Act, Americans with Disabilities Act, or workers' compensation is *not* protected under HIPAA (although this type of information may be protected under other federal or state laws).

**Other allowable uses or disclosures of your health information**

In certain cases, your health information can be disclosed without authorization to a family member, close friend, or other person you identify who is involved in your care or payment for your care. Information about your location, general condition, or death may be provided to a similar person (or to a public or private entity authorized to assist in disaster relief efforts). You'll generally be given the chance to agree or object to these disclosures (although exceptions may be made – for example, if you're not present or if you're incapacitated). In addition, your health information may be disclosed without authorization to your legal representative.

The Plan also is allowed to use or disclose your health information without your written authorization for the following activities:

| | |
|---|---|
| **Workers' compensation** | Disclosures to workers' compensation or similar legal programs that provide benefits for work-related injuries or illness without regard to fault, as authorized by and necessary to comply with the laws |
| **Necessary to prevent serious threat to health or safety** | Disclosures made in the good-faith belief that releasing your health information is necessary to prevent or lessen a serious and imminent threat to public or personal health or safety, if made to someone reasonably able to prevent or lessen the threat (or to the target of the threat); includes disclosures to help law enforcement officials identify or apprehend an individual who has admitted participation in a violent crime that the Plan reasonably believes may have caused serious physical harm to a victim, or where it appears the individual has escaped from prison or from lawful custody |
| **Public health activities** | Disclosures authorized by law to persons who may be at risk of contracting or spreading a disease or condition; disclosures to public health authorities to prevent or control disease or report child abuse or neglect; and disclosures to the Food and Drug Administration to collect or report adverse events or product defects |
| **Victims of abuse, neglect, or domestic violence** | Disclosures to government authorities, including social services or protected services agencies authorized by law to receive reports of abuse, neglect, or domestic violence, as required by law or if you agree or the Plan believes that disclosure is necessary to prevent serious harm to you or potential victims (you'll be notified of the Plan's disclosure if informing you won't put you at further risk) |

| | |
|---|---|
| **Judicial and administrative proceedings** | Disclosures in response to a court or administrative order, subpoena, discovery request, or other lawful process (the Plan may be required to notify you of the request or receive satisfactory assurance from the party seeking your health information that efforts were made to notify you or to obtain a qualified protective order concerning the information) |
| **Law enforcement purposes** | Disclosures to law enforcement officials required by law or legal process, or to identify a suspect, fugitive, witness, or missing person; disclosures about a crime victim if you agree or if disclosure is necessary for immediate law enforcement activity; disclosure about a death that may have resulted from criminal conduct; and disclosure to provide evidence of criminal conduct on the Plan's premises |
| **Decedents** | Disclosures to a coroner or medical examiner to identify the deceased or determine cause of death; and to funeral directors to carry out their duties |
| **Organ, eye, or tissue donation** | Disclosures to organ procurement organizations or other entities to facilitate organ, eye, or tissue donation and transplantation after death |
| **Research purposes** | Disclosures subject to approval by institutional or private privacy review boards, subject to certain assurances and representations by researchers about the necessity of using your health information and the treatment of the information during a research project |
| **Health oversight activities** | Disclosures to health agencies for activities authorized by law (audits, inspections, investigations, or licensing actions) for oversight of the health care system, government benefits programs for which health information is relevant to beneficiary eligibility, and compliance with regulatory programs or civil rights laws |
| **Specialized government functions** | Disclosures about individuals who are Armed Forces personnel or foreign military personnel under appropriate military command; disclosures to authorized federal officials for national security or intelligence activities; and disclosures to correctional facilities or custodial law enforcement officials about inmates |
| **HHS investigations** | Disclosures of your health information to the Department of Health and Human Services to investigate or determine the Plan's compliance with the HIPAA privacy rule |

Except as described in this notice, other uses and disclosures will be made only with your written authorization. For example, in most cases, the Plan will obtain your authorization before it communicates with you about products or programs if the Plan is being paid to make those communications. If we keep psychotherapy notes in our records, in some cases we will obtain your authorization before we release those records. The Plan will never sell your health information unless you have authorized us to do so. You may revoke your authorization as allowed under the HIPAA rules. However, you can't revoke your authorization with respect to disclosures the Plan has already made. You will be notified of any unauthorized access, use or disclosure of your unsecured health information as required by law.

The Plan will notify you if it becomes aware that there has been a loss of your health information in a manner that could compromise the privacy of your health information.

## Your individual rights

You have the following rights with respect to your health information the Plan maintains. These rights are subject to certain limitations, as discussed below. This section of the notice describes how you may exercise each individual right. See the table at the end of this notice for information on how to submit requests.

### Right to request restrictions on certain uses and disclosures of your health information and the Plan's right to refuse

You have the right to ask the Plan to restrict the use and disclosure of your health information for treatment, payment, or health care operations, except for uses or disclosures required by law. You have the right to ask the Plan to restrict the use and disclosure of your health information to family members, close friends, or other persons you identify as being involved in your care or payment for your care. You also have the right to ask the Plan to restrict use and disclosure of health information to notify those persons of your location, general condition, or death – or to coordinate those efforts with entities assisting in disaster relief efforts. If you want to exercise this right, your request to the Plan must be in writing.
The Plan is not required to agree to a requested restriction. If the Plan does agree, a restriction may later be terminated by your written request, by agreement between you and the Plan (including an oral agreement), or unilaterally by the Plan for health information created or received after you're notified that the Plan has removed the restrictions. The Plan may also disclose health information about you if you need emergency treatment, even if the Plan has agreed to a restriction.

An entity covered by these HIPAA rules (such as your health care provider) or its business associate must comply with your request that health information regarding a specific health care item or service not be disclosed to the Plan for purposes of payment or health care operations if you have paid for the item or service, in full out of pocket.

### Right to receive confidential communications of your health information

If you think that disclosure of your health information by the usual means could endanger you in some way, the Plan will accommodate reasonable requests to receive communications of health information from the Plan by alternative means or at alternative locations.

If you want to exercise this right, your request to the Plan must be in writing and you must include a statement that disclosure of all or part of the information could endanger you.

### Right to inspect and copy your health information

With certain exceptions, you have the right to inspect or obtain a copy of your health information in a "designated record set." This may include medical and billing records

maintained for a health care provider; enrollment, payment, claims adjudication, and case or medical management record systems maintained by a plan; or a group of records the Plan uses to make decisions about individuals. However, you do not have a right to inspect or obtain copies of psychotherapy notes or information compiled for civil, criminal, or administrative proceedings. The Plan may deny your right to access, although in certain circumstances you may request a review of the denial.

If you want to exercise this right, your request to the Plan must be in writing. Within 30 days of receipt of your request (60 days if the health information is not accessible onsite), the Plan will provide you with:

- the access or copies you requested;

- a written denial that explains why your request was denied and any rights you may have to have the denial reviewed or file a complaint; or

- a written statement that the time period for reviewing your request will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Plan expects to address your request.

You may also request your health information be sent to another entity or person, so long as that request is clear, conspicuous and specific. The Plan may provide you with a summary or explanation of the information instead of access to or copies of your health information, if you agree in advance and pay any applicable fees. The Plan also may charge reasonable fees for copies or postage. If the Plan doesn't maintain the health information but knows where it is maintained, you will be informed of where to direct your request.

If the Plan keeps your records in an electronic format, you may request an electronic copy of your health information if in a form and format readily producible by the Plan. You may also request that such electronic health information be sent to another entity or person, so long as that request is clear, conspicuous and specific. Any charge that is assessed to you for these copies, if any, must be reasonable and based on the Plan's cost.

**Right to amend your health information that is inaccurate or incomplete**

With certain exceptions, you have a right to request that the Plan amend your health information in a designated record set. The Plan may deny your request for a number of reasons. For example, your request may be denied if the health information is accurate and complete, was not created by the Plan (unless the person or entity that created the information is no longer available), is not part of the designated record set, or is not available for inspection (e.g., psychotherapy notes or information compiled for civil, criminal, or administrative proceedings).

If you want to exercise this right, your request to the Plan must be in writing, and you must include a statement to support the requested amendment. Within 60 days of receipt of your request, the Plan will:

- make the amendment as requested;
- provide a written denial that explains why your request was denied and any rights you may have to disagree or file a complaint; or
- provide a written statement that the time period for reviewing your request will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Plan expects to address your request.

### Right to receive an accounting of disclosures of your health information

You have the right to a list of certain disclosures of your health information the Plan has made. This is often referred to as an "accounting of disclosures." You generally may receive this accounting if the disclosure is required by law, in connection with public health activities, or in similar situations listed in the table earlier in this notice, unless otherwise indicated below. You may receive information on disclosures of your health information for up to six years before the date of your request. You do not have a right to receive an accounting of any disclosures made:

- for treatment, payment, or health care operations;
- to you about your own health information;
- incidental to other permitted or required disclosures;
- where authorization was provided;
- to family members or friends involved in your care (where disclosure is permitted without authorization);
- for national security or intelligence purposes or to correctional institutions or law enforcement officials in certain circumstances; or
- as part of a "limited data set" (health information that excludes certain identifying information).

In addition, your right to an accounting of disclosures to a health oversight agency or law enforcement official may be suspended at the request of the agency or official.

If you want to exercise this right, your request to the Plan must be in writing. Within 60 days of the request, the Plan will provide you with the list of disclosures or a written statement that the time period for providing this list will be extended for no more than 30 more days, along with the reasons for the delay and the date by which the Plan expects to address your request. You may make one request in any 12-month period at no cost to you, but the Plan may charge a fee for subsequent requests. You'll be notified of the fee in advance and have the opportunity to change or revoke your request.

### Right to obtain a paper copy of this notice from the Plan upon request

You have the right to obtain a paper copy of this privacy notice upon request. Even individuals who agreed to receive this notice electronically may request a paper copy at any time.

## Changes to the information in this notice

The Plan must abide by the terms of the privacy notice currently in effect. This notice takes effect on *[date]*. However, the Plan reserves the right to change the terms of its privacy policies, as described in this notice, at any time and to make new provisions effective for all health information that the Plan maintains. This includes health information that was previously created or received, not just health information created or received after the policy is changed. If changes are made to the Plan's privacy policies described in this notice, you will be provided with a revised privacy notice [*describe how revised notice will be provided; e.g., mailed to home address, e-mail*].

## Complaints

If you believe your privacy rights have been violated or your Plan has not followed its legal obligations under HIPAA, you may complain to the Plan and to the Secretary of Health and Human Services. You won't be retaliated against for filing a complaint. To file a complaint, [*describe how to file a complaint, including contact information*].

## Contact

For more information on the Plan's privacy policies or your rights under HIPAA, contact [*name or title of person or office*] at [*telephone number*].

## Additional contacts

The following is a list of key persons or offices you may need to contact to exercise your rights under the HIPAA privacy rule for different benefit plans offered by [VANDERBILT]:

| | **Restricted disclosures** | **Confidential communications** | **Access to or copies of your health information** | **Amendment of your health information** | **Accounting of disclosures** |
|---|---|---|---|---|---|
| [*Plan Name*] | | | | | |
| [*Plan Name*] | | | | | |
| [*Plan Name*] | | | | | |
| [*Plan Name*] | | | | | |

# 10.08 Participant Forms

The following forms are included in this section:

10.08(a) Request for Access to Inspect and Copy

10.08(b) Request to Amend

10.08(c) Request for Restricted Use

10.08(d) Request for Confidential Communications

10.08(e) Request for Accounting of Nonroutine Disclosures

10.08(f) Authorization to Use and/or Disclosure

### *a. Request for Access to Inspect and Copy*

| Instructions for Responding to a Request for Access to Inspect and Copy |
|---|
| **Directions for** VANDERBILT:<br>**Providing Form.** If any person wishes to request access to inspect and copy Personal health plan information, Inspection Contact should provide the person with this Form.<br>**Receiving a Completed Form.** Upon receipt of this Form Inspection Contact should initial and date top right corner and must verify that Part I (Request for Access to Inspect and Copy Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in sections A and B must be marked, and the form must be signed and dated. If the person requesting Personal health plan information is not the subject of the information, Inspection Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03.<br>If Part I is incomplete, Inspection Contact should return it to the person for completion.<br>**Determination of Request.** Upon receipt of this Form with Part I properly completed, Inspection Contact will respond by completing Part II (Determination of Request for Access to Inspect and Copy Personal Health Plan Information, within the timeframes detailed in Section 5.02.<br>Note that although a Designated Record Set includes the Plan's enrollment and Payment information, it does not include VANDERBILT's enrollment and Payment records. |

# Part I - Request for Access to Inspect and Copy Personal Health Plan Information

**Form Received By** | **Date**

With certain exceptions, you have the right to inspect or obtain a copy of your health information in a "Designated Record Set" maintained by the [Health Plan] (the "Plan"). This may include medical and billing records maintained for a health care provider; enrollment, payment, claims adjudication, and case or medical management record systems maintained by a plan; or a group of records the Plan uses to make decisions about individuals. You may request an electronic copy of your health information if it is maintained in an electronic format and the form and format you request is reasonably accessible by the Plan. You may also request that a copy of your health information be sent to another entity or person, so long as that request is clear, conspicuous and specific.

You do not have a right to inspect or obtain copies of psychotherapy notes or information compiled for civil, criminal, or administrative proceedings. In addition, the Plan may deny your right to access, although in certain circumstances you may request a review of the denial.

The Plan may provide you with a summary or explanation of the information in your health plan records instead of access to or copies of your records, if you agree in advance and pay any applicable fees. The Plan may also charge reasonable fees for copies or postage.

| | |
|---|---|
| **1. Employee Name** | **1a. Employee Health Plan ID Number** |
| **1b. Employee Date of Birth** | |
| **2. Name of Person Whose Records You Are Requesting** | **2a. Relationship to Employee**<br>Self ☐ Spouse ☐ Child ☐ Other ☐ |
| **3. Your Name** | **3a. Your Relationship to Person in Box 2**<br>Self ☐ Spouse ☐ Parent ☐ Child ☐<br>☐ **Other (please describe relationship):** |
| **4. Mailing Address for Records** | **4a. City, State, Zip Code** |

**Section A: Requested Personal Records.**

Please identify the personal health plan information in your health plan records you are requesting access to, including the time period to which the information relates:

**Section B: Methods of Access.**

I wish to inspect and copy the personal health plan information described in Section A using the following method(s):

☐ I wish to inspect the records requested in Section A in person. I will arrange a mutually agreeable time to come to the Plan by contacting **[Inspection Contact]**.

☐ I wish to copy the records requested in Section A in person. I will arrange a mutually agreeable time to come to the Plan by contacting **[Inspection Contact].** I understand that I will be charged and I agree to pay the cost of copying at ___ per page.

☐ I wish to have copies of the records requested in Section A sent directly to me, at the address in Box 4. I understand that I will be charged and I agree to pay the cost of copying at ___ per page plus postage.

☐ I wish to have electronic copies of the records requested in Section A that are kept electronically sent directly to me, at the address in Box 4. I understand that I will be charged and I agree to pay the associated cost.

☐ I wish to have copies of the records requested in Section A sent to the following person or entity:_____, at the address in Box 4. I understand that I will be charged and I agree to pay the associated cost.

☐ I wish to have electronic copies of the records requested in Section A that are kept electronically sent to the following person or entity:_____, at the address in Box 4. I understand that I will be charged and I agree to pay the associated cost.

☐ I wish to have the information requested in Section A summarized (instead of receiving the entire record) and sent to me at the address in Box 4. I understand that I will be charged for the summary provided and I agree to pay the cost of preparing the summary, any copying at ___ per page, and postage.

Please return completed form to: **[Inspection Contact]**
**[Contact Address]**
**[Contact Phone Number]**

| **VANDERBILT** | **Date** |
|---|---|

# Part II - Determination of Request for Access to Inspect and Copy Personal Health Plan Records

**Form Part II Prepared By** | **Date Part II Issued**

After reviewing your request for access to inspect and/or copy personal health plan records, Inspection Contact has made the following determination **[check one (1)]**:

☐ **Request granted** (see Section A below).

☐ **Request partially granted and partially denied** (see Section A and B or C below).

☐ **Request denied with no right to review** (see Section B below).

☐ **Request denied with right to review** (see Section C below).

### Section A: Request Granted

Your request for access to inspect and/or copy personal health plan records is granted **[in full / in part]. [All / Some] of the** health information you requested is available to you for inspection or copying, or both. If you requested to review the records in person, please contact **[Inspection Contact]** at **[Phone Number]** to coordinate this request. If you requested that the records or a summary be sent to you, a copy is attached.

### Section B: Request Denied with No Right to Review

Your request for access to inspect and copy personal health plan records is denied **[in full / in part]** for the following reasons **[check all that apply]**:

☐ The information requested is psychotherapy notes.

☐ The information is for civil, criminal, or administrative proceedings.

☐ The information is created for research and you agreed to forgo access while the research is in progress.

☐ The information is subject to the Privacy Act, 5 U.S.C. 522(a) and access may be denied under that law. [**include only if Plan Sponsor is federal agency or contractor]**

☐ The information was obtained from someone other than a health care provider under a promise of confidentiality and access would reveal the source.

☐ The information requested is not maintained by the Plan. Inspection Contact does not know who maintains the specific information requested.

☐ The information requested is not maintained by the Plan. The information is maintained by _____. Please contact them for access to the information.

### Section C: Request Denied with Right to Review

Your request for access to inspect and/or copy personal health plan records has been denied **[in full / in part]** because a licensed health care professional has determined that the access is reasonably likely to endanger an individual. You have a right to ask the Plan to have the denial reviewed by another licensed health care professional.

If you wish to ask the Plan to review this denial, please send a written request to **[Inspection Contact]**, **[Inspection Contact Title]** at **[Contact Location]**. For more information, please contact **[Inspection Contact]**, at [Contact Telephone Number].

If you have been denied access to inspect and copy PHI, you may complain to the Plan or to the Secretary of the U.S. Department of Health and Human Services at http://www.hhs.gov/ocr/privacyhowtofile.htm For more information, please contact **[Complaint Manager] at [Complaint Manager's Telephone Number].**

**Name of Plan Representative** | **VANDERBILT of Plan Representative** | **Date of Determination**

### *b. Request to Amend Personal Health Plan Information*

| Instructions for Responding to a Request for Access to Inspect and Copy |
|---|
| **Directions for** VANDERBILT:<br>**Providing Form.** If any person wishes to request that the Plan amend his or her personal health plan information, Amendment Contact should provide the person with this Form.<br>**Receiving a Completed Form**. Upon receipt of this Form, Amendment Contact must verify that Part I (Request to Amend Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in each section must be marked, and the Form must be signed and dated. If the person requesting personal health plan information is not the subject of the information, Amendment Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03.<br>If Part I of the Form is incomplete, Amendment Contact should return it to the person for completion.<br>**Determination of Request.** Upon receipt of this Form with Part I properly completed, Amendment Contact will respond by completing Part II (Determination of Request to Amend Personal Health Plan Information), within the timeframes detailed in Section 5.03. |

# Part I - Request to Amend Personal Health Plan Information

**Form Received By** | **Date**

With certain exceptions, you have a right to request that the Plan amend your health information in a "Designated Record Set." The Plan may deny your request for a number of reasons. For example, your request may be denied if the health information is accurate and complete; was not created by the Plan (unless the person or entity that created the information is no longer available); is not part of the Designated Record Set; or would not be available for inspection (e.g., psychotherapy notes or information compiled for civil, criminal or administrative proceedings).

| | |
|---|---|
| **1. Employee Name** | **1a. Employee Health Plan ID Number** |
| **1b. Employee Date of Birth** | |
| **2. Name of Person Whose Records You Are Requesting** | **2a. Relationship to Employee**<br>Self ☐ Spouse ☐ Child ☐ Other ☐ |
| **3. Your Name** | **3a. Your Relationship to Person in Box 2**<br>Self ☐ Spouse ☐ Parent ☐ Child ☐<br>☐ **Other (please describe relationship):** |
| **4. Mailing Address for Records** | **4a. City, State, Zip Code** |

I request that the Plan amend the following information in a personal health plan record **[describe the information that is the subject of the Amendment request]**:

_____

_____

_____

_____

The identified information should be amended because:

_____

_____

_____

I understand that if the Plan approves my request to amend a health plan record, the Plan will not necessarily delete the original information in the Designated Record Set, but instead may choose to identify the information in the Designated Record Set(s) that is the subject of my request for Amendment and provide a link to the location of the Amendment.

**VANDERBILT** | **Date**

## Part II - Determination of Request to Amend Personal Health Plan Information

| Form Part II Prepared By | Date Part II Issued |
|---|---|
| | |

☐ Request Approved

☐ Request Denied for the following reasons **[check all that apply]**:

- ☐ The PHI or record was not created by the Plan.
- ☐ The PHI or record is not part of one of the Plan's Designated Record Sets.
- ☐ The PHI or record is not available for inspection under the HIPAA Privacy Rule.
- ☐ The PHI or record is accurate and complete referring.

If your request has been denied, you have the right to submit a statement of disagreement and the basis for such disagreement (limited to five (5) pages) to **[Amendment Contact]** at **[Amendment Location]**. In response, **[Amendment Contact]** will send you a copy of any rebuttal statement that is prepared. If you submit a statement of disagreement, when the Plan makes future disclosures of your disputed PHI or record, a copy of your request, the denial, and any disagreement and rebuttal will be attached to the disclosed PHI or record.

If your request has been denied and you choose not to submit a statement of disagreement, you may still ask the Plan to include a copy of your Amendment and the denial along with any future disclosures of the health information that is the subject of the Amendment request.

If you have been denied access to inspect and copy PHI, you may complain to the Plan or to the Secretary of the U.S. Department of Health and Human Services at http://www.hhs.gov/ocr/privacyhowtofile.htm For more information, please contact **[Complaint Manager]** at **[Complaint Manager's Telephone Number].**

| Name of Plan Representative | VANDERBILT of Plan Representative | Date of Determination |
|---|---|---|
| | | |

### c. Restricted Access

| Instructions for Responding to a Request for Restricted Use of PHI |
|---|
| **Directions for** VANDERBILT:<br>**Providing Form**. If any person wishes to request that the Plan restrict or terminate a restriction on the Plan's use and disclosure of his or her PHI, Restriction Contact should provide the person with this Form.<br>**Receiving a Completed Form**. Upon receipt of this Form, Restriction Contact must verify that Part I (Request for Restricted Use Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in each section must be marked, and the form must be signed and dated. If the person requesting the restricted use of PHI is not the subject of the PHI, Restrictions Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03.<br>If Part I of the Form is incomplete Restriction Contact should return it to the person for completion.<br>**Determination of Request for Restricted Use of PHI**. When Part I, Section A has been completed, Restriction Contact will respond by completing Part II (Determination of Request for Restricted Use of Personal Health Plan Information), in accordance with the Plan's policy detailed in Section 5.04.<br>**Terminating a Restriction**. *Agreed Upon by a Participant (Part I, Section B).* When Part I, Section B, of the Form has been completed, Restriction Contact will not send a completed Part II (Determination of Request for Restricted Use of Personal Heath Plan Information), as detailed in Section 5.04.<br>**Terminating a Restriction.** *Not Agreed Upon by a Participant (Part III).* The Plan will only complete Part III of the Form to provide notice to a person (or the person's representative) that the Plan will terminate a previously agreed upon restriction, without the person's approval (except for agreements regarding out-of-pocket payments as described in Section 5.04). The Plan will complete Part III on the original Form (where the restriction was requested and approved), as detailed in Section 5.04. Such restriction is effective only with respect to PHI created or received after the Plan has provided notice of the termination to the person. |

# Part I - Request for Restricted Use of Personal Health Plan Information

**Form Received By** | **Date**

You have the right to ask the Plan to restrict the use and disclosure of your health information for Treatment, Payment, or Health Care Operations, except for uses or disclosures required by law. You have the right to ask the Plan to restrict the use and disclosure of your health information to family members, close friends, or other persons you identify as being involved in your care or Payment for your care. You also have the right to ask the Plan to restrict use and disclosure of health information to notify those persons of your location, general condition, or death — or to coordinate those efforts with entities assisting in disaster relief efforts. If you want to exercise this right, your request to the Plan must be in writing.

The Plan is not required to agree to a requested restriction. If the Plan does agree, a restriction may later be terminated by your written request, by agreement between you and the Plan (including an oral agreement), or unilaterally by the Plan for health information created or received after you're notified that the Plan has removed the restrictions. The Plan may also disclose your health information if you need emergency Treatment, even if the Plan has agreed to a restriction.

| | |
|---|---|
| **1. Employee Name** | **1a. Employee Health Plan ID Number** |
| **1b. Employee Date of Birth** | |
| **2. Name of Person Whose Records You Are Requesting** | **2a. Relationship to Employee**<br>Self ☐ Spouse ☐ Child ☐ Other ☐ |
| **3. Your Name** | **3a. Your Relationship to Person in Box 2**<br>Self ☐ Spouse ☐ Parent ☐ Child ☐<br>☐ **Other (please describe relationship):** |
| **4. Mailing Address for Records** | **4a. City, State, Zip Code** |

**Section A: Request to Restrict Use and Disclosure of Personal Health Plan Information**

I request that the use and disclosure of personal health plan information for the person in Box 2 be restricted in the manner described below:

_____

_____

_____

☐ I have / ☐ I have not : already paid the health care provider in full for the items or services related to this information.

I understand that the Plan may deny this request. I also understand that the Plan may remove this restriction in the future if I am notified in advance.

**Section B: Request to Terminate Restricted Use and Disclosure of Personal Health Plan Information**

☐ I request that the restriction on the use and disclosure of personal health plan information made on _____**[Date Initial Request Made]** be terminated. I understand that upon receipt of this form, the Plan will terminate the previously accepted restriction. Once a restriction has been terminated, the Plan will use and disclose personal health plan information as permitted or required by law.

☐ I agreed orally to terminate the restricted use and disclosure of personal health plan information belonging to the person in Box 2 made on _____**[Date Initial Request Made]**. This serves as formal documentation of that oral agreement.

**VANDERBILT** | **Date**

## Part II - Determination of Request for Restricted Use of Personal Health Plan Information

| Form Part II Prepared By | Date Part II Issued |
|---|---|
| | |

After reviewing your request to restrict use of personal health plan information, the Plan has made the following determination [check one (1)]:

☐ Request Approved

☐ Request Denied

| Name of Plan Representative | VANDERBILT of Plan Representative | Date of Determination |
|---|---|---|
| | | |

## Part III - Termination of a Request for Restricted Use of Personal Health Plan Information

| Form Part III Prepared By | Date Part III Issued |
|---|---|
| | |

The Plan is providing you with notice that it is terminating its agreement to restrict its use and disclosure of personal health plan information as documented above in Part II of this Form. Any personal health plan information created or received on or after **[Date of Mailing]** will not be subject to the restriction. The Plan may use and disclose your personal health plan information as permitted by law.

| Name of Plan Representative | VANDERBILT of Plan Representative | Date of Determination |
|---|---|---|
| | | |

## *d. Request for Confidential Communications*

| Instructions for Responding to a Request for Confidential Communications |
|---|
| **Directions for** VANDERBILT:<br>**Providing Form.** If any person wishes to request that the Plan use an alternative means to communicate his or her personal health plan information or that he or she receive personal health plan information at an alternate location, Communication Contact should provide the person with this Form. Examples of alternative means could include mail instead of fax, phone instead of mail, etc.<br>**Receiving a Completed Form**. Upon receipt of this Form, Communication Contact must verify that Part I (Request for Confidential Communications of Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in each section must be marked, and the form must be signed and dated. If the person requesting the Confidential Communications of personal health plan information is not the subject of the information, Restrictions Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03.<br>If Part I of the Form is incomplete, Communication Contact should return it to the person for completion.<br>**Determination of Request**. Upon receipt of this Form with Part I properly completed, Communication Contact will respond by completing Part II (Determination of Request for Confidential Communications of Personal Health Plan Information), within the timeframes detailed in Section 5.05 of the Manual. |

# Part I - Request for Confidential Communications of Personal Health Plan Information

**Form Received By** | **Date**

If you think that disclosure of your health information by the usual means could endanger you in some way, the Plan will accommodate reasonable requests to receive communications of health information from the Plan by alternative means or at alternative locations. If the Payment of benefits is affected by this request, the Plan may also deny this request unless you contact the Communication Contact to discuss alternative Payment means.

| | |
|---|---|
| **1. Employee Name** | **1a. Employee Health Plan ID Number** |
| **1b. Employee Date of Birth** | |
| **2. Name of Person Whose Records You Are Requesting** | **2a. Relationship to Employee**<br>Self ☐ Spouse ☐ Child ☐ Other ☐ |
| **3. Your Name** | **3a. Your Relationship to Person in Box 2**<br>Self ☐ Spouse ☐ Parent ☐ Child ☐<br>☐ **Other (please describe relationship):** |
| **4. Mailing Address for Records** | **4a. City, State, Zip Code** |

I am requesting that communication of personal health plan information for the person in Box 2 be provided by alternative means or at alternative locations. I **[check one (1)] [ ☐ am ☐ am not]** making this request because disclosure of all or part of the information to which the request pertains could endanger me, or the person I represent.

Please send the information by the following alternative means:

_____

_____

_____

Please send the information to the following alternative address, if different than address above:

**Street address** _____

**City, State and ZIP** _____

**Phone** _____

**Other** _____

If this request relates to communication regarding Payment for health care services, please indicate how we can reach you to discuss alternative Payment means.

_____

**VANDERBILT** | **Date**

# Part II - Determination of Request for Confidential Communications of Personal Health Plan Information

**Form Part II Prepared By** | **Date Part II Issued**

After reviewing your request for Confidential Communications of personal health plan information, the Plan has made the following determination [check one (1)]:

☐ Request Approved

☐ Request Denied

**Section A: Request Approved**

The Plan accepts your written request for the use of alternative means or alternative locations for Confidential Communications of personal health plan information The Plan will send personal health plan information **[check all that apply]**:

☐ By the alternative means you specified in Part I; and/or

☐ To the alternative address you specified in Part I.

**Section B: Request Denied**

The Plan denies your written request for the use of alternative means or alternative locations for Confidential Communications of personal health plan information for the following reasons **[check all that apply]**:

☐ The Plan has determined that the request is incomplete.

☐ The Plan has determined that the request is not reasonable

☐ The request does not clearly state that the Plan's usual means or locations of disclosure of personal health plan information poses a danger to you (or to the person in Box 2).

**Name of Plan Representative** | **VANDERBILT of Plan Representative** | **Date of Determination**

## e. Accounting of Non-routine Disclosures

| Instructions for Responding for Accounting of Nonroutine Disclosures of PHI |
|---|
| **Directions for** VANDERBILT:<br>**Providing Form**. If any person wishes to request an accounting of non-routine PHI disclosures, Disclosure Contact should provide the person with this Form and a copy of the Privacy Notice detailing the non-routine disclosures.<br>**Receiving a Completed Form.** Upon receipt of this Form, Disclosure Contact must verify that Part I (Request for Accounting of Non-routine Disclosures of Personal Health Plan Information) has been properly completed. To be properly completed, the appropriate boxes in each section must be marked, and the form must be signed and dated. If the person requesting personal health plan information is not the subject of the information, Disclosure Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03.<br>If part I of the Form is incomplete, Disclosure Contact should return it to the person for completion.<br>**Determination of Request**. Upon receipt of the Form with Part I properly completed, Disclosure Contact will respond by completing Part II (Determination of Request for Accounting of Non-routine Disclosures of Personal Health Plan Information), within the timeframes detailed in Section 5.06 of the Manual.<br>If the Plan is required to temporarily suspend a person's right to receive an accounting, as detailed in Section 5.06, Disclosure Contact must provide the person requesting the accounting with the appropriate information after the suspension of this person's right to receive the accounting has been lifted. |

# Part I - Request for Accounting of Non-routine Disclosures of Personal Health Plan Information

**Form Received By** **Date**

You have the right to a list of certain disclosures the **[Health Plan]** (the "Plan") has made of your health information. This is often referred to as an "accounting of disclosures." You generally may receive an accounting of disclosures if the disclosure is required by law, in connection with public health activities, or in similar situations as described in more detail in the Plan's Privacy Notice.

| | |
|---|---|
| **1. Employee Name** | **1a. Employee Health Plan ID Number** |
| **1b. Employee Date of Birth** | |
| **2. Name of Person Whose Accounting You Are Requesting** | **2a. Relationship to Employee**<br>Self ☐ Spouse ☐ Child ☐ Other ☐ |
| **3. Your Name** | **3a. Your Relationship to Person in Box 2**<br>Self ☐ Spouse ☐ Parent ☐ Child ☐<br>☐ **Other (please describe relationship):** |
| **4. Mailing Address for Records** | **4a. City, State, Zip Code** |

I understand that I can request an accounting of non-routine disclosures of personal health plan information once within any twelve (12)-month period, free of charge. If I request accountings more frequently, I understand the Plan will charge me a reasonable, cost-based fee for each subsequent request.

The accounting of non-routines disclosures of PHI will include the following information:

- The date of disclosure;
- The name of the person or entity to whom information was made and the person's or entity's address (if known);
- A brief description of the information disclosed; and
- The reason for the disclosure.

I hereby request an accounting of any non-routine disclosures of personal health plan information of the person named in Box 2 made by the Plan for the following time period _____ **[Enter time period (disclosures can be requested for a time period of up six (6) years)].**

**VANDERBILT** **Date**

# Part II - Determination of Request for Accounting of Non-routine Disclosures of Personal Health Plan Information

**Form Part II Prepared By** | **Date Part II Issued**

After reviewing your request for an accounting of non-routine disclosures of personal health plan information, the Plan has made the following determination **[check one(1)]**:

☐ Request Approved without a fee (see section A below)

☐ Request Approved with a fee (see section B below)

☐ Request Denied (see section C below)

**Section A: Request Approved without a Fee**

Your request for an accounting of non-routine disclosures of personal health plan information is approved.

Your requested accounting of disclosures is attached to this form. There is no charge for processing request.

**Section B: Request Approved with a Fee**

Your request for an accounting of non-routine disclosures of personal health plan information is approved.

You requested and received an accounting of non-routine disclosures of personal health plan information, free of charge on **[Insert date that last free of charge accounting was disclosed]**. The charge for processing this request is $_____ **[Insert fee],** as a fee for the preparation of your request for an accounting. You have the right to withdraw or modify your request for an accounting. Unless you contact **[Disclosure Contact]** at the following address **[Disclosure Contact Address]** within 10 days from _____ **[Insert date]** to withdraw or modify your request, **[Disclosure Contact]** will mail you your requested accounting and will send you a bill for $_____ which you agreed to pay by signing Part I of this form.

**Section C: Request Denied**

Your request for an accounting of non-routine disclosures of personal health plan information is denied because none of your PHI was disclosed for a non-routine purpose.

If you wish to make a complaint, please contact **[Complaint Manager]** at **[Telephone Number].**

**Name of Plan Representative** | **VANDERBILT of Plan Representative** | **Date of Determination**

## *f. Authorization for Use and/or Disclosure of Health Information*

| **Directions for** VANDERBILT **for Using Model Authorization Form** |
|---|
| **Providing Form.** If any person wishes to request an Authorization for the use or disclosure of PHI in the **[Name of Plan]**, Authorization Contact should provide the person with this Form.<br><br>**Receiving a Completed Form.** Upon receipt of this Form Authorization Contact should initial and date the top right corner and must verify that the Form has been properly completed.<br><br>If the person submitting the Form is not the subject of the PHI, Authorization Contact should verify the identity and authority of the person and follow the procedures detailed in Section 3.03.<br><br>This model Authorization Form is intended to allow a person to have health information sent from VANDERBILT's health plan (including its Business Associates, Insurers and HMOs) to a third party for non-health plan purposes, including VANDERBILT.<br><br>[VANDERBILT may want to modify the specific options described in Sections A – D of this Form to reflect the most common types of requests that occur for its plans. VANDERBILT may want to delete the option in Section C that permits the Plan to be paid for using PHI in marketing activities or selling PHI to a third party if VANDERBILT does not expect to use PHI in that manner.]<br><br>The "Your Rights" section includes optional language. The first option assumes Payment, Treatment, enrollment, and eligibility decisions are not conditioned on the signing of an Authorization. The second option says the Plan may require Authorizations prior to a person's enrollment to make enrollment/eligibility determinations or underwriting or risk rating determinations. The appropriate option should be selected, to reflect VANDERBILT's practices.<br><br>VANDERBILT could also amend this Form to be used by VANDERBILT or an individual in requesting PHI from another covered entity in cases when an Authorization is required (either by the HIPAA privacy rule or that Covered Entity). However, the other Covered Entity is likely to require the use of its own Authorization Form.<br><br>This model Authorization Form complies with the requirements of the Health Insurance Portability and Accountability Act (HIPAA). State laws may impose additional requirements. VANDERBILT should review this form and state law issues with counsel. |

**Instructions for the Individual Completing this Authorization Form**

- The **[Health Plan]** ("Plan") cannot use or disclose your health information (or the health information of your children or other people on whose behalf you can act) for certain purposes without your Authorization. This form is intended to meet the Authorization requirement.
- You must respond to each section, and sign and date this form, in order for the Authorization to be valid.
- If you wish to authorize the use and/or disclosure of any notes the Plan may have that were taken by a mental health professional at a counseling session, along with other health information, you must complete one (1) form for the counseling session notes and one (1) separate form for other health information.
- The sample responses given for each section below are not exhaustive and are meant for illustrations only. Under HIPAA, there are no limitations on the information that can be authorized for disclosure.

**Section A: Health Information to be Used or Released.** Describe in a specific and meaningful way the information to be used or released. Example descriptions include medical records relating to my appendectomy, my laboratory results and medical records from **[date]** to **[date]**, or the results of the MRI performed on me in July 1998.

**Section B: Person(s) Authorized to Use and/or Receive Information.** Provide a name or specific identification of the person, class of persons, or organization(s) authorized to use or receive the health information described in Section A.

**Section C: Purpose(s) for which Information will be Used or Released.** Describe each purpose for which the information will be used or released. If you initiate the Authorization and do not wish to provide a statement of purpose, you may select "at my request."

**Section D: Expiration.** Specify when this Authorization will expire. For example, you may state a specific date, a specific period of time following the date you signed this Authorization Form, or the resolution of the dispute for which you've requested assistance.

**VANDERBILT Line.** If you are authorizing the release of somebody else's health information, then you must describe your authority to act for the Individual.

# Authorization to Use and/or Disclose Personal Health Plan Information

**Form Received By** **Date**

| **1. Employee Name** | **1a. Employee Health Plan ID Number** |
|---|---|
| **1b. Employee Date of Birth** | |
| **2. Name of Person Whose Health Information is the Subject of this Authorization** | **2a. Relationship to Employee**<br>Self ☐ Spouse ☐ Child ☐ Other ☐ |
| **3. Your Name** | **3a. Authority**<br>If you are not the person in Box 2, please describe your authority to act on his or her behalf: |
| **4. Mailing Address for Records** | **4a. City, State, Zip Code** |

I hereby authorize **[Health Plan]** ("Plan") to use and/or disclose the health information described in Sections A – E below.
**[Alternative for** VANDERBILT: **modify this section to specify the organization that will release the information on behalf of the Plan, such as Insurer, HMO, Business Associate, or** VANDERBILT**]**

**Section A: Health Information to be Used and/or Disclosed**

Specify the health information to be released and/or used, including (if applicable) the time period(s) to which the information relates. Select only one (1) of the following boxes:

☐ All of my past, present or future health claims and/or medical records.

☐ All of my health information relating to Claim Number _____or care rendered on _____.

☐ Other (please specify): _____

**Section B: Person(s) Authorized to Use and/or Receive Information**

Specify the persons or class of persons authorized to use and/or receive the health information described in Section A:

_____

**Section C: Purposes for Which Information will be Used or Disclosed**

Specify each purpose for which the health information described in Section A may be used or disclosed. Select all of the applicable boxes below:

☐ To facilitate the resolution of a claim dispute.

☐ As part of my application for leave of under the Family and Medical Leave Act (FMLA) or state family leave laws.

☐ For a disability coverage determination.

☐ For sales or marketing activities when the Plan is receiving remuneration from a third party.

☐ At my request.

☐ Other (please specify):_____

**Section D: Expiration of Authorization**

Specify when this Authorization expires. (Provide a date or triggering event related to the use or disclosure of the information.)

☐ On the following date: _____.

☐ Upon the passage of the following amount of time: _____.

☐ Upon my disenrollment from VANDERBILT's health plan.

☐ Upon my return from FMLA leave.

☐ Other (please specify): _____

_____

**Your rights:**

- You can revoke this Authorization at any time by submitting a written revocation to [Authorization Contact] at the following address: _____
- A revocation will not apply to information that has already been used or disclosed in reliance on the Authorization.
- Once the information is disclosed pursuant to this Authorization, it may be redisclosed by the recipient and the information will no longer be protected by HIPAA.
- [**Option 1: The Plan may not condition Treatment, Payment, enrollment or eligibility for benefits on whether I sign the Authorization.]**
- **[Option 2: This clause applies to individuals not yet enrolled in the Plan. If this Authorization was requested so the Plan can make an eligibility or enrollment determination or an underwriting or risk rating determination, then the person in Box 2 may be ineligible for enrollment or benefits if you fail to sign this form.]**
- You will be provided with a copy of this Authorization Form, after signing, if **the Plan** sought the Authorization.

_____ _____

**VANDERBILT** **Date**

# 10.09 Breach Report Forms

The following forms are included in this section:

10.09(a) Breach Incident Report Form

10.09(b) Breach Incident Log

## *a. Breach Incident Report Form*

| **Directions for** VANDERBILT **for Using Breach Incident Report Form** |
|---|
| **Use of Form.** As described in Section 4.07, the Plan must investigate incidents of impermissible access, uses, or disclosures of PHI which may compromise the privacy or security of the information. The purpose of this Form 10.09(a) is to collect facts about such confirmed or potential incidents. VANDERBILT workforce members aware of such incidents use this Form 10.09(a) to submit information to the Breach Contact, or use it as a guide to an oral conversation when disclosing relevant facts to the Breach Contact upon discovery of an incident requiring urgent intervention.<br><br>**Receiving a Completed Form.** Upon receipt of this Form the Breach Contact (or his or her designee) should initial and date the top right corner and must verify that the Form has been properly completed. All reported incidents should be investigated and the applicable procedures detailed in Section 6.05 followed to completion.<br><br>This model Breach Incident Report Form captures the types of information needed to initiate the mitigation requirements of the Health Insurance Portability and Accountability Act (HIPAA). State laws may impose additional information gathering or mitigation measures. |

# Breach Incident Report Form

**Form Received By** **Date**

Please fill out this Form completely and send to the following VANDERBILT official who has been designated as the Plan's Breach Contact. If the incident is ongoing or otherwise requires immediate intervention, please call the Breach Contact at the telephone number provided:

[Name/Title or both]; [email address and faVANDERBILTmile number] with a copy to [email address and faVANDERBILTmile number]; [telephone number]. In the case of an incident requiring urgent intervention, if the Breach Contact is travelling or unavailable, please contact [Name/Title or both] at [telephone number].

## Section A:

| | |
|---|---|
| **1. Reporting Staff Member Name** | **1a. Staff Member Daytime Telephone Number** |
| **1b. Staff Member Department/Geographical Location** | |
| **2. Is this a confirmed or suspected breach?**<br>☐ Confirmed ☐ Suspected | **2a. Is this an ongoing breach?**<br>☐ Yes ☐ No |
| **3. Do you believe this to be an intentional or an accidental use or disclosure?**<br>☐ Intentional ☐ Accidental | **3a. Please estimate the number of individuals whose PHI might be affected**<br>☐ 500 or more ☐ Fewer than 500<br>**More specific estimate number, if possible:**<br>_____ |
| **4. Date the incident was discovered**<br>_____<br>MM / DD / YY | **4a. Date (or date range) the incident occurred**<br>_____ _____<br>Starting MM/DD/YY Ending MM/DD/YY |

**Section B: Type of Breach**

Select the type of breach incident you are reporting. If selecting the "Other" category, provide a short description in the blank field at the end of this section B **[check all that apply]**:

- ☐ Theft
- ☐ Loss
- ☐ Improper Disposal
- ☐ Unauthorized Access
- ☐ Hacking/IT Incident
- ☐ Unknown
- ☐ Other

Please describe "Other" _____

**Section C: Location of Breached Information**

Select the location of the PHI at the time of the breach. If selecting the "Other" category, provide a short description in the blank field at the end of this section C **[check all that apply]**:

- ☐ Laptop
- ☐ Desktop Computer
- ☐ Network Server
- ☐ E-mail
- ☐ Other portable electronic device
- ☐ Electronic medical record
- ☐ Paper
- ☐ Other

Please describe "Other" _____

**Section D: Type of PHI Involved in the Breach**

Select the type of PHI involved in the breach. If selecting the "Other" category, provide a short description in the blank field at the end of this section D **[check all that apply]**:

- ☐ Demographic information
- ☐ Financial information
- ☐ Clinical information
- ☐ Other

Please describe "Other" _____

**Section E: Brief Description of the Breach**

Please summarize the breach incident, including the geographical area and the specific IT systems/servers/applications involved, as well as any information about internal or external parties involved in the incident:

_____

_____

_____

_____

_____

_____

### *b. Breach Incident Log*

| Directions for VANDERBILT for Using Breach Incident Log |
| --- |
| **Use of Form.** VANDERBILT workforce members use this Form 10.09(b) to record information about breach incidents reported to VANDERBILT affecting, or suspected of affecting, the Plan's PHI. The log is updated as the Breach Contact (or his or her designee) investigate breach incidents and implement the mitigation procedures described in Section 6.05.<br><br>This model Breach Incident Log captures the types of information needed to document the breach incidents reported by workforce members of VANDERBILT and submit relevant information to HHS about logged incidents for which a submission is required. This log is designed to address breach documentation needs under the Health Insurance Portability and Accountability Act (HIPAA). State laws may impose additional information gathering or documentation measures. |

**Plan Year _____**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Event # | Event Date or Range | Date Event Discovered | Approx. # of People Affected | Type of Event | Location of Event | Type of PHI Involved in Event | Safeguards in Place Before Event | Actions Taken in Response to Event | Date(s) Individual Notice Provided | Was Substitute Notice Required | Date Provided Media Notice | Date Incident Reported to HHS | Notice Exception Applied to Incident[5] |
| | m/d/y | m/d/y | x,xxx | √ all applicable | √ all applicable | √ all applicable | √ all applicable | √ all applicable | m/d/y or N/A | Y/N | m/d/y or N/A | m/d/y or N/A | √ all applicable |
| 1 | | | | ☐ Theft<br>☐ Loss<br>☐ Improper Disposal<br>☐ Unauthorized Access<br>☐ Hacking/IT Event<br>☐ Unknown<br>☐ Other[1] | ☐ Laptop<br>☐ Desktop Computer<br>☐ Network Services<br>☐ Email<br>☐ Other Portable Electronic Device<br>☐ Electronic Medical Record<br>☐ Paper<br>☐ Other[2] | ☐ Demographic Information<br>☐ Financial Information<br>☐ Clinical Information<br>☐ Other[3] | ☐ Firewalls<br>☐ Packet Filtering<br>☐ Secure Browser Sessions<br>☐ Strong Authentication<br>☐ Encrypted Wireless<br>☐ Physical Security<br>☐ Logical Access Control<br>☐ Antivirus Software<br>☐ Intrusion Detection<br>☐ Biometrics | ☐ Enhanced Security and/or Privacy Safeguards<br>☐ Mitigation of Resulting Harm<br>☐ Sanctions of Relevant Workforce members<br>☐ Enhanced Policies and Procedures<br>☐ Other[4] | | | | | ☐ Affected data in "secured" format<br>☐ Unintentional access or use by staff or Business Associate meeting required conditions<br>☐ Inadvertent disclosure meeting required conditions<br>☐ Data could not be retained<br>☐ Low probability of compromise to the data or information |

[1] Explain Column E "Other": _____

[2] Explain Column F "Other": _____

[3] Explain Column G "Other": _____

[4] Explain Column I "Other": _____

[5] Attach explanatory analyses for exceptions relied on Column N (see Section 6.05(b)): _____

| A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Event #** | **Event Date or Range** | **Date Event Discovered** | **Approx. # of People Affected** | **Type of Event** | **Location of Event** | **Type of PHI Involved in Event** | **Safeguards in Place Before Event** | **Actions Taken in Response to Event** | **Date(s) Individual Notice Provided** | **Was Substitute Notice Required** | **Date Provided Media Notice** | **Date Incident Reported to HHS** | **Notice Exception Applied to Incident[5]** |
| | m/d/y | m/d/y | x,xxx | √ all applicable | √ all applicable | √ all applicable | √ all applicable | √ all applicable | m/d/y or N/A | Y/N | m/d/y or N/A | m/d/y or N/A | √ all applicable |
| **2** | | | | ☐ Theft<br>☐ Loss<br>☐ Improper Disposal<br>☐ Unauthorized Access<br>☐ Hacking/IT Event<br>☐ Unknown<br>☐ Other[1] | ☐ Laptop<br>☐ Desktop Computer<br>☐ Network Services<br>☐ Email<br>☐ Other Portable Electronic Device<br>☐ Electronic Medical Record<br>☐ Paper<br>☐ Other[2] | ☐ Demographic Information<br>☐ Financial Information<br>☐ Clinical Information<br>☐ Other[3] | ☐ Firewalls<br>☐ Packet Filtering<br>☐ Secure Browser Sessions<br>☐ Strong Authentication<br>☐ Encrypted Wireless<br>☐ Physical Security<br>☐ Logical Access Control<br>☐ Antivirus Software<br>☐ Intrusion Detection<br>☐ Biometrics | ☐ Enhanced Security and/or Privacy Safeguards<br>☐ Mitigation of Resulting Harm<br>☐ Sanctions of Relevant Workforce members<br>☐ Enhanced Policies and Procedures<br>☐ Other[4] | | | | | | ☐ Affected data in "secured" format<br>☐<br>☐ Unintentional access or use by staff or Business Associate meeting required conditions<br>☐ Inadvertent disclosure meeting required conditions<br>☐ Data could not be retained<br>☐ Low probability of compromise to the data or information |

[1] Explain Column E "Other": _____

[2] Explain Column F "Other": _____

[3] Explain Column G "Other": _____

[4] Explain Column I "Other": _____

[5] Attach explanatory analyses for exceptions relied on Column N (see Section 6.05(b)): _____

# 10.10 Legally Required Uses, Public Health Activities, Other Situations Not Requiring Authorization

As described in Section 4, the Plan, its Insurers and Business Associates should, without obtaining a Participant's Authorization, use and disclose PHI if required by law, for certain public health purposes, and in other similar situations, described in the following chart:

| Purpose for disclosure | Permissible disclosures of PHI |
|---|---|
| Workers' compensation | • Includes disclosures of PHI to workers' compensation or similar legal programs that provide benefits for work-related injuries or illness without regard to fault, as authorized by and necessary to comply with such laws. |
| Necessary to prevent or lessen serious threat to health or safety | • Includes disclosures of PHI to a person or persons if made under good faith belief that releasing PHI is necessary to prevent or lessen a serious and imminent threat to public or personal health or safety if made to someone reasonably able to prevent or lessen the threat (including disclosures to the target of the threat).<br>• Includes disclosures of PHI to assist law enforcement officials in identifying or apprehending an individual because the individual has made a statement admitting participation in a violent crime that the Plan reasonably believes may have caused serious physical harm to a victim, or where it appears the individual has escaped from prison or from lawful custody. |
| Public health activities | • Includes disclosures of PHI authorized by law to persons who may be at risk of contracting or spreading a disease or condition.<br>• Includes disclosures of PHI to public health authorities to prevent or control disease and to report child abuse or neglect.<br>• Includes disclosures of PHI to the FDA to collect or report adverse events or product defects. |
| Victims of abuse, neglect, or domestic violence | • Includes disclosures of PHI to government authorities, including social services or protected services agencies authorized by law to receive reports of abuse, neglect, or domestic violence, as required by law or if the subject of the PHI agrees or the Plan believes disclosure is necessary to prevent serious harm to the individual or potential victims; the Plan will notify the individual that is the subject of the disclosure if it won't put the individual at further risk. |

| Purpose for disclosure | Permissible disclosures of PHI |
|---|---|
| Judicial and administrative proceedings | • Includes disclosures of PHI in response to a court or administrative order; and disclosures in response to a subpoena, discovery request or other lawful process (the Plan is required to notify the individual that is the subject of the request for PHI of the request, or to receive satisfactory assurance from the party seeking the PHI that efforts were made to notify the individual that is the subject of the request for PHI or to obtain a qualified protective order concerning the PHI). |
| Law enforcement purposes | • Includes disclosures of PHI to law enforcement officials as required by law or pursuant to legal process, or to identify a suspect, fugitive, witness or missing person.<br>• Includes disclosures of PHI about a crime victim if the individual that is the subject of the PHI agrees or if disclosure is necessary for immediate law enforcement activity.<br>• Includes disclosures of PHI regarding a death that may have resulted from criminal conduct and disclosures to provide evidence of criminal conduct on the Plan's premises.<br>• For any PHI that potentially relates to Reproductive Health Care, PHI may not be disclosed without a valid attestation from the official requesting the use or disclosure. |
| Health oversight activities | • Includes disclosures of PHI to health agencies for activities authorized by law (audits, inspections, investigations, or licensing actions) for oversight of the health care system, government benefits programs for which health information is relevant to beneficiary eligibility, compliance with regulatory programs, or civil rights laws. Any PHI that potentially relates to Reproductive Health Care may not be disclosed without a valid attestation from the person requesting the use or disclosure. |
| Decedents: Coroners and Medical Examiners | • Includes disclosures of PHI to a coroner or medical examiner to identify the deceased or to determine the cause of death. Any PHI that potentially relates to Reproductive Health Care may not be disclosed without a valid attestation from the person requesting the use or disclosure. |
| Decedents: Funeral Directors | • Includes disclosures of PHI to funeral directors to carry out their duties. |
| Organ, eye, or tissue donation | • Includes disclosures of PHI to organ procurement organizations or other entities to facilitate cadaveric organ, eye, or tissue donation and transplantation. |

| Purpose for disclosure | Permissible disclosures of PHI |
|---|---|
| Research purposes | • Includes disclosures of PHI subject to approval by institutional or privacy boards, and subject to certain assurances and representations by researchers regarding necessity of using PHI and treatment of PHI during a research project. |
| Specialized government functions | • Includes disclosures of PHI of individuals who are Armed Forces personnel or foreign military personnel under appropriate military command authority.<br>• Includes disclosures to authorized federal officials for national security or intelligence activities.<br>• Includes disclosures to correctional facilities or custodial law enforcement officials about inmates. |
| Department of Health and Human Services (HHS) Investigations | • Includes disclosures of PHI to HHS to investigate or determine the Plan's compliance with the HIPAA Privacy Rule. |

# 10.11 Attestation

ATTESTATION FOR A REQUESTED USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION POTENTIALLY RELATED TO REPRODUCTIVE HEALTH CARE PROHIBITED PURPOSES

[INSTRUCTIONS AND *ATTESTATION BEGIN ON FOLLOWING PAGE*]

**[Name of Plan]**

| Attestation Received By | Date |
|---|---|
| | |

# Instructions

**Purpose**

When the [Name of Plan] (the "Plan") or its Business Associate receives a request for protected health information (PHI) potentially related to reproductive health care, it must obtain a signed attestation that clearly states the requested use or disclosure is not for the prohibited purposes described below, where the request is for PHI for any of these purposes:

Health oversight activities
Judicial or administrative proceedings
Law enforcement
Regarding decedents, disclosures to coroners and medical examiners.

**Prohibited Purposes**. The Plan and its Business Associates may not use or disclose PHI to:

(1) conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating lawful reproductive health care,

(2) impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating lawful reproductive health care, or

(3) identify any person for any purpose described in (1) or (2).

The prohibition applies when the reproductive health care at issue (1) is lawful under the law of the state in which the health care is provided under the circumstances in which it is provided, (2) is protected, required, or authorized by Federal law, including the United States Constitution, under the circumstances in which the health care is provided, regardless of the state in which it is provided, or (3) is provided by another person and presumed lawful.

**Information for the Person Requesting the PHI**

By signing this attestation, you are verifying that you are not requesting PHI for a prohibited purpose and acknowledging that criminal penalties may apply if untrue.

You may not add content that is not required or combine this form with another document except where another document is needed to support your statement that the requested disclosure is not for a prohibited purpose. For example, if the requested PHI is potentially related to reproductive health care that was provided by someone other than the Plan or its Business Associate from whom you are requesting the PHI, you may submit a document that supplies information that demonstrates a substantial factual basis that the reproductive health care in question was not lawful under the specific circumstances in which it was provided.

This attestation document may be provided in electronic format, and electronically signed by the person requesting protected health information when the electronic signature is valid under applicable Federal and state law.

**Information for the Plan or Business Associate**

The Plan or Business Associate may not rely on the attestation to disclose the requested PHI if any of the following is true:

It is missing any required element or statement or contains other content that is not required.
It is combined with other documents, except for documents provided to support the attestation.
The Plan or Business Associate knows that material information in the attestation is false.
A reasonable covered entity or business associate in the same position would not believe the requestor's statement that the use or disclosure is not for a prohibited purpose as described above.

If the Plan or Business Associate later discovers information that reasonably shows that any representation made in the attestation is materially false, leading to a use or disclosure for a prohibited purpose as described above, it must stop making the requested use or disclosure.

The Plan or Business Associate may not make a disclosure if the reproductive health care was provided by another person and the requestor indicates that the PHI requested is for a prohibited purpose as described above, unless the requestor supplies information that demonstrates a substantial factual basis that the reproductive health care was not lawful under the specific circumstances in which it was provided.

The Plan or Business Associate must obtain a new attestation for each specific use or disclosure request.

The Plan or Business Associate must maintain a written copy of the completed attestation and any relevant supporting documents.

# Attestation

*The entire form must be completed for the attestation to be valid.*

**1. Name of person(s) or specific identification of the class of persons to receive the requested PHI.**

**2. Name or other specific identification of the person or class of persons from whom you are requesting the use or disclosure.**

**3. Description of specific PHI requested, including name(s) of individual(s), if practicable, or a description of the class of individuals, whose protected health information you are requesting.**

I attest that the use or disclosure of PHI that I am requesting is *not* for a purpose prohibited by the HIPAA Privacy Rule at
45 CFR 164.502(a)(5)(iii) because (check one box):

☐ The purpose of the use or disclosure of protected health information is *not* to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care or to identify any person for these purposes.

☐ The purpose of the use or disclosure of protected health information *is* to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care, or to identify any person for those purposes, but the reproductive health care at issue was *not lawful* under the circumstances in which it was provided.

I understand that I may be subject to criminal penalties pursuant to 42 U.S.C. 1320d-6 if I knowingly and in violation of
HIPAA obtain individually identifiable health information relating to an individual or disclose individually identifiable health information to another person.

**Signature of the person requesting the PHI** **Date**

*If you have signed as a representative of the person requesting PHI, provide a description of your authority to act for that person.*

Please return completed attestation to the Privacy Official:

Julie Hanna
Benefits Operations Manager
Vanderbilt University – People Experience
PMB #407704
2301 Vanderbilt Place
Nashville, TN 37240-7704
615-343-6624
Julie.Hanna@Vanderbilt.edu