Bioventus HIPAA Privacy Policies and Procedures

Bioventus Policy POL-000064 [A]

bioventus

\

Table of Contents

Contents

I. HIPAA General Compliance Policy

A. Introduction to HIPAA Compliance Policies and Procedures

Bioventus and its subsidiaries and affiliates, including Bioness and Misonix (collectively **"Bioventus"**), have adopted these Bioventus HIPAA Privacy Policies and Procedures (**"Policies"**) to comply with HIPAA, where "HIPAA" is broadly defined as the Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act)(ARRA), and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013), and the HIPAA Privacy, Breach Notification, and Security Rules.

Bioventus has a duty and responsibility to protect the privacy and security of Individually Identifiable Health Information (**"IIHI")** generally, and Protected Health Information (**"PHI"**), as defined by HIPAA, both in its role as a HIPAA Covered Entity and a HIPAA Business Associate, each defined below. Bioventus adopts these Policies to comply with its various HIPAA requirements.

B. Scope of HIPAA Policies and Procedures

These Policies govern HIPAA privacy compliance for the Bioventus workforce. Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers who encounter IIHI and PHI in the course of their work with Bioventus (the **"workforce"**) must read, understand, and comply with these Policies.

C. HIPAA General Policy Statement

Bioventus complies with all the requirements of HIPAA and fully documents all HIPAA compliance-related activities and efforts, in accordance with our HIPAA Documentation Retention Policy, set forth below. These Policies are intended to be read in conjunction with Bioventus's information security policies and procedures.

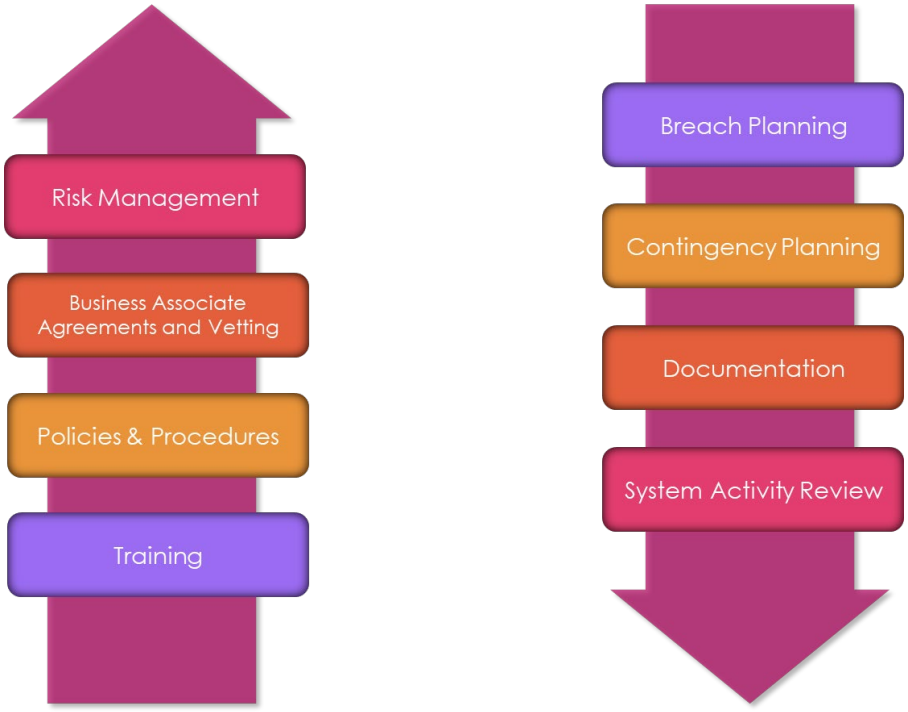
D. Overview of HIPAA Procedures

Bioventus commits to enacting, supporting, and maintaining the following procedures and activities, as required by HIPAA:

- **Privacy Policies and Procedures**: Bioventus will develop, implement, and maintain up-to-date written privacy policies and procedures that are consistent with HIPAA.
  Privacy Personnel: Bioventus has designated a HIPAA Privacy Officer responsible for developing and implementing its privacy policies and procedures.
    - Bioventus' HIPAA Privacy Officer is:
      Katrina Church Pope
      SVP, Chief Compliance Officer
      Bioventus
      Direct Phone: 919-474-6758
      Mobile Phone: 336-543-7242
      Email: katrina.church@bioventus.com
    - Bioventus' HIPAA Security Officer is:
      James Ellis
      Director, IT Security, Risk & Compliance

Bioventus
Direct Phone: 919-886-4968
Mobile Phone: 336-255-9277
Email: james.ellis@bioventus.com

- **Workforce Training and Management**: Bioventus will train all workforce members who may encounter IIHI or PHI on its HIPAA policies and procedures, as necessary and appropriate for the workforce members to carry out their various functions.
- **Sanctions**: Bioventus will apply appropriate sanctions against workforce members who violate its HIPAA policies or applicable law.
- **Mitigation**: Bioventus will mitigate any harmful effect it learns was caused by the use or disclosure of PHI by its workforce or its Business Associates in violation of its privacy policies and procedures or HIPAA.
- **Data Safeguards**: Bioventus will maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional uses or disclosures of PHI in violation of HIPAA and its own policies, and to limit incidental uses and disclosures.
- **Complaints**: Bioventus will establish procedures for individuals to complain about its compliance with its privacy policies and procedures and HIPAA and will explain those procedures in its Notice of Privacy Practices and other related privacy notices.
- **Non-Retaliation and Waiver**: Bioventus will not retaliate against a person for exercising HIPAA rights, for assisting in an investigation by HHS or another appropriate authority as required by law, or for opposing an act or practice that the person believes in good faith violates any HIPAA standard or requirement. Bioventus will not require an individual to waive any HIPAA right as a condition for obtaining treatment, payment, enrollment, or benefits eligibility.
- **Documentation and Record Retention**: For at least six years after the later of the date of their creation or last effective date, Bioventus will maintain its privacy policies and procedures, its privacy practices notices, dispositions of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.
- **HIPAA Compliance Continuous Process Flow**



E. HIPAA Compliance and Enforcement

All Bioventus managers and supervisors are responsible for enforcing these Policies. Workforce members who violate these Policies and procedures are subject to discipline up to and including termination in accordance with Bioventus' HIPAA Sanctions Policy and general HR policies and procedures. Sanctions can include but are not limited to specific retraining, verbal warnings, written warnings, performance improvement plans, and termination.

II. HIPAA Definitions Policy

The following definitions apply to these Policies. If a term is not defined below, but is defined by HIPAA, the HIPAA statutory and regulatory definitions apply:

- **"Business Associate"** means an individual or business that creates, receives, maintains, or transmits Protected Health Information (**"PHI"**) on behalf of a Covered Entity to provide services to the Covered Entity (*e.g.,* IT vendors, data analysts, management companies, attorneys, consultants). When Bioventus agrees to function as a Business Associate, it must enter into a Business Associate Agreement (**"BAA"**). If a workforce member is unsure whether Bioventus is acting as a Business Associate in a current or proposed business process, that workforce member will contact the HIPAA Privacy Officer for guidance.
- **"BAA"** or **"Business Associate Agreement"** means a contract between a HIPAA Covered Entity and a Business Associate that addresses the core issues related to protecting the privacy and security of PHI related to the Business Associate relationship.
- **"Covered Entity"** means a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction. Bioventus is considered a HIPAA Covered Entity for Exogen billing purposes. The two most prevalent types of Covered Entities are (1) Health care providers, and companies like Bioventus acting on their behalf, that engage in certain electronic transactions such as billing insurance companies (*e.g.,* health systems, hospitals, physician practices, pharmacies), and (2) health plans (*e.g.,* health insurance carriers, employer group health plans, Medicare, Medicaid).
- **"De-Identified"** data means health information that does not identify an individual, where there is no reasonable basis to believe that the information can be used to identify the individual. Data is not de-identified if it can be reasonably combined with other data to re-identify an individual. HIPAA establishes a very strict standard for de-identifying data. To de-identify data without involving a statistician, (1) none of the 18 identifiers listed in the definition of PHI can be included in the data set, and (2) the data set cannot be used (either alone or in combination with other information) to identify the individual. Simply removing identifiers like patient names and addresses from a PHI data set is often not enough to render the information "de-identified" and therefore it will remain subject to HIPAA. For example, a record is PHI and not "de-identified" if it contains data elements such as zip code, any element of a date (except the year) that relates to the patient (*e.g.,* date of service, admission date, birth date), or medical record number. Any workforce member seeking to de-identify data must first consult with and receive approval from the HIPAA Privacy Officer.
- **"Exogen"** is Bioventus' Ultrasound Bone Healing System which uses safe, painless, low-intensity ultrasound waves to amplify a person's body's natural bone repair processes. Bioventus is

considered a Covered Entity under HIPAA for Exogen because Bioventus bills government payors and private insurance on behalf of health care providers for Exogen.

- **"HHS"** or **"Health and Human Services"** means the U.S. Department of Health and Human Services, the federal agency that has overall responsibility for implementing HIPAA.
- **"HIPAA"** or the **"Health Insurance Portability and Accountability Act"** was enacted to protect the privacy and security of patient health information. Certain state laws also protect patient information. HIPAA is comprised of 3 key rules: Privacy Rule, Breach Notification Rule, and Security Rule. HIPAA applies to PHI in the hands of Covered Entities or their Business Associates
- **"HIPAA Authorization"** or **"HIPAA Authorization Form"** means a patient's written authorization permitting the use or disclosure of PHI. In many cases, a workforce member cannot use or disclose PHI without first obtaining a HIPAA Authorization from the patient permitting the use or disclosure. If you receive a HIPAA Authorization Form or want to use one, contact Bioventus' HIPAA Privacy Officer. See **Addendum H: HIPAA Authorization Form - Sample** for a sample HIPAA Authorization Form.
- **"HIPAA Breach Notification Rule"** means if Bioventus experiences a PHI breach, it may be required to notify affected individuals, HHS, and, in some cases, the media. Generally, a breach is an unpermitted use or disclosure of unsecured PHI under the HIPAA Privacy Rule that compromises the security or privacy of PHI. **If you suspect a potential HIPAA Breach, you must notify the HIPAA Privacy Officer immediately.**
- **"HIPAA Privacy Rule"** sets national standards for the use and disclosure of PHI. The Privacy Rule protects PHI held or transmitted by a Covered Entity or its Business Associate, in any form, whether electronic, paper, or verbal.
- **"HIPAA Security Rule"** sets standards for information security requirements for PHI, which are designed to protect:
    - Confidentiality (*i.e.,* PHI cannot be available or disclosed to unauthorized persons or processes);
    - Integrity (*i.e.,* PHI cannot be altered or destroyed in an unauthorized manner); and
    - Availability (*i.e.,* PHI must be accessible and usable on demand by authorized persons).

  Bioventus will develop reasonable and appropriate IT security policies, analyze security risks to PHI in its environment, and implement appropriate controls to secure PHI.
- **"IIHI"** or **"Individually Identifiable Health Information"** means a subset of health information, including demographic information collected from an individual, that:
    - Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
        - (a) Relates to the physical or mental health or condition of an individual; or
        - (b) The provision of health care to an individual; or
        - (c) The payment for the provision of health care to an individual; and
    - Identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.
- **"Incident Response"** means Bioventus' response to the potential or actual impermissible use or disclosure of PHI.
- **"Minimum Necessary Rule"** or **"Minimum Necessary Standard"** applies to uses and disclosures of PHI that are permitted under the HIPAA Privacy Rule and means workforce members may only use or disclose the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure, or request.
- **"Patient Rights"** means patients' rights under HIPAA to request:
    - Access to their PHI;
    - An amendment to their PHI;

- An accounting of certain disclosures of their PHI;
- Confidential communications that include their PHI; and
- Restrictions on certain uses and disclosures of their PHI.

Some state laws afford patients additional rights concerning their health information (*e.g.,* California patients may have the right to have an addendum added to their medical records). If you receive a request from a patient or a customer related to any of these rights, forward the request to Bioventus' HIPAA Privacy Officer for review and response.

- **"PHI"** or **"Protected Health Information"** is information that (1) identifies an individual, and (2) relates to the health or condition of the individual, the individual's receipt of health care services or products, or payment by insurers or the government for those health care services or products. PHI may take several forms, including (1) verbal (*e.g.,* conversations with a physician's office staff or insurance company), (2) written information (*e.g.,* patient files, forms, charge sheets), or (3) electronic information (*e.g.,* patient information contained in emails, servers, mobile devices, cloud storage). PHI includes demographic information about a patient (*e.g.,* name, address, DOB) tied to a Covered Entity. There does not need to be specific information about the individual's health for the information to be PHI (*e.g.,* a list of a doctor's patients). Any 1 (or more) of 18 identifiers make information "identifiable," including:

Graphic courtesy of: https://careprovider.org/wp-content/uploads/List-of-PHI.png

III. HIPAA Documentation Retention Policy

A. HIPAA Documentation Policy Statement

- Bioventus retains HIPAA-related documentation for a minimum period of six years after the date of its creation or modification, or the date when it was last in effect, whichever is later.

- HIPAA-related documentation is securely stored and maintained in a manner consistent with HIPAA.
- HIPAA-related documentation is available to those workforce members who have a legitimate need for it and are authorized to access it.
- Where Bioventus maintains HIPAA-related documentation as a Business Associate, it complies with the documentation retention provisions of the applicable BAA.

B. General Guidance on Required HIPAA Documentation

Bioventus is a HIPAA Covered Entity for Exogen billing purposes. HIPAA requires that Covered Entities maintain the documentation specified in Section C below. Where Bioventus is a HIPAA Business Associate, the BAA may define document retention periods. Where BAAs are silent as to document retention, Bioventus will follow the HIPAA six-year rule.

C. Documents Required for HIPAA

HIPAA documentation includes at least the following:

- HIPAA policies and procedures;
- HIPAA risk analyses/assessments and related notes and research materials;
- IIHI or PHI disclosures accounting documentation which includes (1) information required in any accounting (*e.g.,* dates of disclosures, name of entity receiving disclosures, description), (2) the written accounting that is provided to the individual, and (3) the titles of the persons responsible for receiving and processing requests for an accounting by individuals;
- PHI amendment documentation, including amendment requests and supplemental material received, such as statements of disagreement and rebuttal statements, approval, or denial notices;
- All complaints received and their disposition, if any;
- All BAAs, other contracts, and addenda to existing contracts with Business Associates and limited data set users, as well as amendments, renewals, revisions, and terminations;
- The names and titles of the HIPAA Privacy and Security Officers and person responsible for receiving complaints and providing information on the Notice(s) of Privacy Practices;
- Training provided (*i.e.,* topics, dates, and participants);
- Sanctions imposed against non-complying workforce members;
- All versions of the Notice(s) of Privacy Practices and any signed acknowledgments;
- The methods and results of analyses that justify any release(s) of de-identified information, where required by HIPAA;
- Agreed-to restrictions on uses and disclosures of information and terminations of such restrictions;
- Access documentation (including the designated record sets subject to access by individuals), the titles of the persons responsible for receiving and processing requests for access by individuals, access approval/denial notices, and requests for review;
- The titles of the persons responsible for receiving and processing requests for PHI amendments by individuals;
- All signed authorizations and revocations;
- All approved confidential communication requests and terminations or revocations; and
- All materials related to a HIPAA Breach investigation and response.

D. Practical Implementation of HIPAA Documentation Retention

Bioventus will retain electronic copies of HIPAA-related documentation in approved records repositories, such as SharePoint, OneDrive, and Exogen Direct. HIPAA-related documentation will not be maintained on individual computers or devices and will not be stored in email. Hard copy PHI will be maintained in locked file cabinets. After six years, if there is no information or litigation hold, and the PHI is not needed for another legitimate business need, it must be deleted and/or shredded pursuant to Department of Defense destruction guidance.

IV. HIPAA Investigations Policy

A. HIPAA Investigations Policy Statement

Bioventus cooperates with HIPAA-related investigations conducted by HHS or its Office of Civil Rights (**"OCR"**) as required by law. The HIPAA Privacy Officer is the primary liaison between Bioventus and government officials.

B. HIPAA Investigations Procedures

Workforce members who are designated to assist with HIPAA-related investigations conducted by HHS must adhere to the following procedures:

- Whenever an HHS investigation is discovered, the following persons must be notified as soon as possible:
  - HIPAA Privacy Officer;
  - General Counsel;
  - Chief Executive Officer;
  - Chief Compliance Officer;
  - Director, Internal Audit;
  - VP of Global Information Systems; and
  - VP Patient Access & Reimbursement;
- Cooperate, but do not volunteer information or records that are not requested;
- Kindly ask for the official government agency-issued I.D. of the investigators (business cards are NOT official identification). Write down their names, office addresses, telephone numbers, fax numbers, and email addresses. If investigators cannot produce acceptable I.D. upon reasonable

request, call legal counsel immediately and defer the provision of confidential information until after you confer with counsel or until the investigators produce acceptable I.D.;

- Accompany the investigators to the room internally designated for them to wait in while the necessary Bioventus workforce members are notified. Anyone who has reception or front desk duties should be trained to know the location of the internally designated room to accompany the investigators to;
- Have at least one, if not two, individuals present during discussions with the investigators to document the requests made to the investigators and the answers provided by the investigators;
- Determine if there are any law enforcement personnel present (*i.e.,* FBI, US Attorney investigators, State Prosecutor investigators, etc.). If law enforcement personnel are present, then the investigation is likely a criminal one, with much more severe penalties than may result from a civil investigation. Generally, guns strapped to hips are a good indicator of the presence of law enforcement personnel; but, if in doubt, ask;
- If law enforcement is present, someone from the General Counsel's office must be present as well, if possible;
- Once I.D. is verified, designated workforce members may permit the investigators to access PHI, in accordance with Bioventus' Notice of Privacy Practices (**"NPP"**), HIPAA policies and procedures, and federal and state law.
    - Once investigators have verified their identities and have also verified their authority to access PHI, it is a violation of HIPAA to withhold PHI from them if the PHI sought is the subject matter of the investigation or reasonably related to the investigation.
    - It is appropriate to ask investigators to verify that they are seeking access to PHI because it is directly related to legitimate investigatory purposes and document their responses in your own written records;
- Have at least one, if not two, individuals present when inquiring about authority to access PHI and the use the investigators will make of the PHI being requested. All witnesses will prepare a written summary of the conduct and communications they observed as soon as possible after the incident; these summaries must be annotated with the time and date of the event, the time and date that the summaries were completed, and the witnesses' signatures;
- Limit investigator interactions with non-designated employees. There is no requirement that Bioventus provide witnesses to be questioned during an initial phase of an investigation. The burden is on the government to ask to speak with specific individuals;
- Do NOT instruct employees to hide or conceal facts, or otherwise mislead investigators;
- Ask the investigators for documents related to the investigation. For example, request:
    - Copies of any search warrants and/or entry and inspection orders;
    - Copies of any complaints;
    - A list of patients they are interested in; and
    - A list of documents/items seized;
- Do not expect that investigators will necessarily provide any of the above, except for the search warrant and a list of documents/items seized (if any);
- Do not leave the investigators alone, if possible. Assign someone to assist each investigator present;
- Do not offer the investigators food (coffee or water is allowed). Don't do anything that could be construed as a "bribe" or a "kickback" to induce favorable treatment, such as offering to buy the investigators lunch or Starbucks; and
- Tell investigators what you are required by law to tell them. Answer direct questions fully and to the best of your ability. Always defer to the advice of legal counsel if you are unsure of what or how much to say.

See **Addendum A**: **HHS list of items and people that may be requested, examined, or interviewed during an investigation** for an HHS list of items and interviews that may be requested, examined, or interviewed in a HIPAA investigation.

V. HIPAA Breach Notification Policy

A. Scope of HIPAA Breach Notification Policy

This HIPAA Breach Notification Policy governs HIPAA breach notification for the Bioventus workforce and is intended to be read in conjunction with all other Bioventus data breach related policies and procedures, (*e.g.,* the Bioventus Information Security Incident Response Plan, and applicable BAAs). If any conflicts between policies arise, these Policies will control with respect to PHI and IIHI.

B. HIPAA Breach Notification Introduction

HIPAA breach notification obligations apply to "unsecured" electronic PHI that has not been "secured" (*i.e.,* encrypted) according to HHS (**"U.S. Department of Health and Human Services"**) and NIST (**"National Institute of Standards and Technology"**) standards. PHI that has been secured by these standards, or fully de-identified, and is subject to unauthorized access or another act that would constitute a "breach," does not invoke any notification requirements under this Policies.[1]

The HIPAA Breach Notification Rule may require that Bioventus notify individual patients, medical provider customers, BAA counterparties, and various governmental regulators including HHS and, in some cases, state Attorneys General.

C. HIPAA Breach Notification Policy Statement

- A HIPAA breach is any intentional or unintentional unauthorized acquisition, access, use, or disclosure of unsecured PHI, in a manner not permitted by HIPAA that compromises the security or privacy of PHI,[2] unless there is a:
  - **Low probability of compromise**. There is no HIPAA breach if, as set forth in the procedures below, Bioventus can demonstrate there is a low probability that the PHI was compromised (a breach is presumed by law and the burden is on Bioventus to show a low probability of compromise);
  - **Good faith employee exception**. There was an unintentional acquisition, access, or use of PHI by a person acting under Bioventus' authority, made in good faith, within the scope of that authority, that does not result in further violation of the rules; or
  - **3rd party retention exception**. Bioventus has a good faith belief that the person to whom PHI was improperly disclosed would not reasonably be able to retain such information.
- Bioventus provides timely breach notifications to affected legal or natural person(s) and/or government regulators, as required by law.

---

[1] This HIPAA breach notification encryption exception does not apply to paper, film, and other hardcopy PHI, because these materials cannot be electronically encrypted (protected) in their native forms.

[2] The terms "acquisition" and "access" are not defined; however, the Data Breach Notification Rule commentary states that the terms should be taken in their ordinary meaning and encompassed within the meanings of "use" and "disclosure," which are defined. "Use" is "sharing, employment, application, utilization, examination, or analysis of [PHI] within an entity that maintains such information." "Disclosure" is the "release, transfer, provision of access to, or divulging in any exceptions, is a breach."

- A breach is treated as "discovered" by Bioventus on the first day on which the breach is known or should reasonably have been known to any employee or agent of Bioventus.[3]
- The HIPAA Privacy Officer manages breach notification investigations, determinations, and responses, including the determination of whether a notifiable breach has occurred.
- Bioventus notifies and cooperates with law enforcement where a suspected HIPAA breach may involve criminal wrongdoing, either on the part of an unknown threat actor or a malicious insider.
- Bioventus provides required notifications without unreasonable delay and no later than 60 days from discovery of the HIPAA breach, unless law enforcement requests a delay in writing.
- If law enforcement requests a delay in notification, Bioventus will provide notification promptly after the law enforcement delay is lifted.
- See **Addendum B: Model HIPAA Breach Notification Letter Template from the American Health Information Management Association** for a Model HIPAA Breach Notification Letter Template from the American Health Information Management Association.
- See **Addendum C: Business Associate Security Incident Notification Letter Template** for a Business Associate Security Incident Notification Letter Template.

D. HIPAA Breach Notification Procedures

- **Workforce members will immediately report all potential breaches to the HIPAA Privacy Officer:** All workforce members who suspect a HIPAA breach must notify the HIPAA Privacy Officer in person, by phone, and/or at katrina.church@bioventus.com immediately. When in doubt, workforce members will err on the side of contacting the HIPAA Privacy Officer.
- **HIPAA Privacy Officer Reporting:** The HIPAA Privacy Officer must, as soon as practicable, notify the following in the event of a potentially reportable HIPAA breach:
  - General Counsel;
  - Chief Executive Officer;
  - Chief Compliance Officer;
  - Director, Internal Audit;
  - VP of Global Information Systems; and
  - VP Patient Access & Reimbursement.
- **Mitigating potential breaches**: Bioventus will take action to mitigate any HIPAA breach as soon as it occurs. For example, workforce members will immediately delete misdirected information, close electronic files containing PHI accessed in error, and request the return of and deletion of PHI sent to an incorrect recipient, along with written confirmation that no further disclosure will be made. If the HIPAA breach is significant and requires further mitigation, the HIPAA Privacy Officer, the VP of Information Technology, and the General Counsel, along with additional subject matter experts as necessary, will coordinate on proper additional mitigation measures.
- **Investigating potential breaches**: The HIPAA Privacy Officer will promptly investigate all reported potential HIPAA breaches to determine whether there has been an actual "breach" of PHI under HIPAA and these Policies. The investigation will consider, at minimum, the nature and extent of the PHI impacted, the number of potentially impacted patients and practices, the type of unauthorized disclosure, the nature of the threat actor (where applicable), steps taken to mitigate harm to patients, and steps taken to reduce the risk of a similar event in the future.

[3] If a Bioventus workforce member maliciously causes a HIPAA Breach, Bioventus becomes aware of the HIPAA Breach when it knows or reasonably should have known of the malicious act. In other words, Bioventus is not necessarily "aware" of a HIPAA Breach committed by a malicious insider who hides their conduct, on the date the insider acted.

- **Determining whether a "breach" occurred**: To determine whether a HIPAA breach has occurred, the HIPAA Privacy Officer must consider:
    - **Whether the breach involved PHI:** Did the incident involve individually identifiable information concerning a patient's health, health care, or payment for health care, including financial account information? If so, it might be a HIPAA breach if the other elements are met.
    - **Whether it violates the HIPAA Privacy Rule:** Were the uses or disclosures made without authorization and not subject to one of the exceptions set forth above? If so, it might be a HIPAA breach if the other elements are met.
    - **Whether there is a low probability of compromise:** If the prior two elements are met, a HIPAA breach is presumed by operation of law. Bioventus may determine, however, that no notifiable HIPAA breach occurred if, considering all the relevant factors, including at least the following, there is a low probability of compromise:
        - The nature and extent of the PHI involved;
        - The unauthorized person who used, accessed, or received the PHI;
        - Whether the information was acquired or viewed; and
            - *Note: OCR takes the position that unauthorized encryption of PHI due to ransomware results in PHI being "acquired" by the threat actor.*
        - The extent to which the risk to the information has been mitigated, including whether there is a low probability of harm to individuals.
    - **Documentation:** Bioventus will maintain documentation of its breach determination analysis for at least six years, including specifically documenting the analysis of exceptions to the HIPAA Breach Notification Rule, and any risk assessments demonstrating a low probability of compromise.
- **Notice - In General**: HIPAA breach notices must include a brief description of what happened, a description of the types of PHI involved, steps affected individuals should take to protect themselves from potential harm, a brief description of the actions taken in response to the breach, and contact procedures for the individuals to ask questions. Breach notices must be written in plain language and easy to understand. See **Addendum B: Model HIPAA Breach Notification Letter Template from the American Health Information Management Association** for a Model HIPAA Breach Notification Letter Template.
- **Insurance**: The HIPAA Privacy Officer will coordinate with the General Counsel to determine if cyber insurance notification requirements are triggered by a HIPAA breach.
- **Immediate Notice:** If the HIPAA Privacy Officer reasonably believes that information is subject to immediate misuse, the HIPAA Privacy Officer may provide immediate notice to the patient by telephone or other means, and then follow up with the required formal notification requirements described below.
- **Notification by Mail**: The HIPAA Breach Notification Rule requires notice to be provided to patients by First Class Mail, where possible. If Bioventus has insufficient or outdated contact information for 10 or more individuals, Bioventus will provide substitute individual notice by either posting the notice on its website home page for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside, as described below. If Bioventus has incorrect or outdated mailing address information for fewer than 10 individuals, telephone or email may be used to contact patients, so long as the notification is documented in writing by the HIPAA Privacy Officer at the time notice is made.
- **Substitute Notice**: In most cases, Bioventus may only use email to notify patients if specifically requested by an individual, or substitute notice via the website or local print or broadcast media

if Bioventus does not have current contact information for fewer than 10 impacted patients. When using substitute notice, Bioventus must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach.

- **Business Associate Notification**: Bioventus will require all Business Associates to notify it immediately in the event the Business Associate becomes aware of a security incident involving PHI. Business Associates will be required, to the extent possible, to identify each person whose information was breached and provide the information necessary to allow Bioventus to comply with its HIPAA breach notification obligations. Bioventus will review and comply with its own BAAs in the event of triggering security incidents or breaches of unsecured PHI.
- **"Small" HIPAA Breaches (500 or fewer patients):** If a HIPAA breach involves the PHI of fewer than 500 people, Bioventus may either report it to HHS immediately or Bioventus can maintain a log of such breaches and submit the log to HHS annually within 60 days of the end of the calendar year at this website:
  - https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true
- **Notice to HHS (500 or more patients impacted)**: Bioventus must notify major media outlets and HHS of a breach affecting more than 500 people, prior to or simultaneous with notifying impacted patients. Notices to HHS of HIPAA breaches involving more than 500 people are made at this website:
  - https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true
  - Note that even though notice must be made without delay, HHS provides a form to update notices with newly discovered information. These submissions are posted publicly on the HHS website.
- **Media Notice**: If a breach of PHI involves more than 500 residents in a state, Bioventus must notify prominent media outlets in that state. The notice will be provided without unreasonable delay but no later than 60 days after discovery of the breach.
- Bioventus will review these Policies at least annually and revise them, as needed. Where appropriate, Bioventus will sanction workforce members whose conduct contributed to a HIPAA breach.

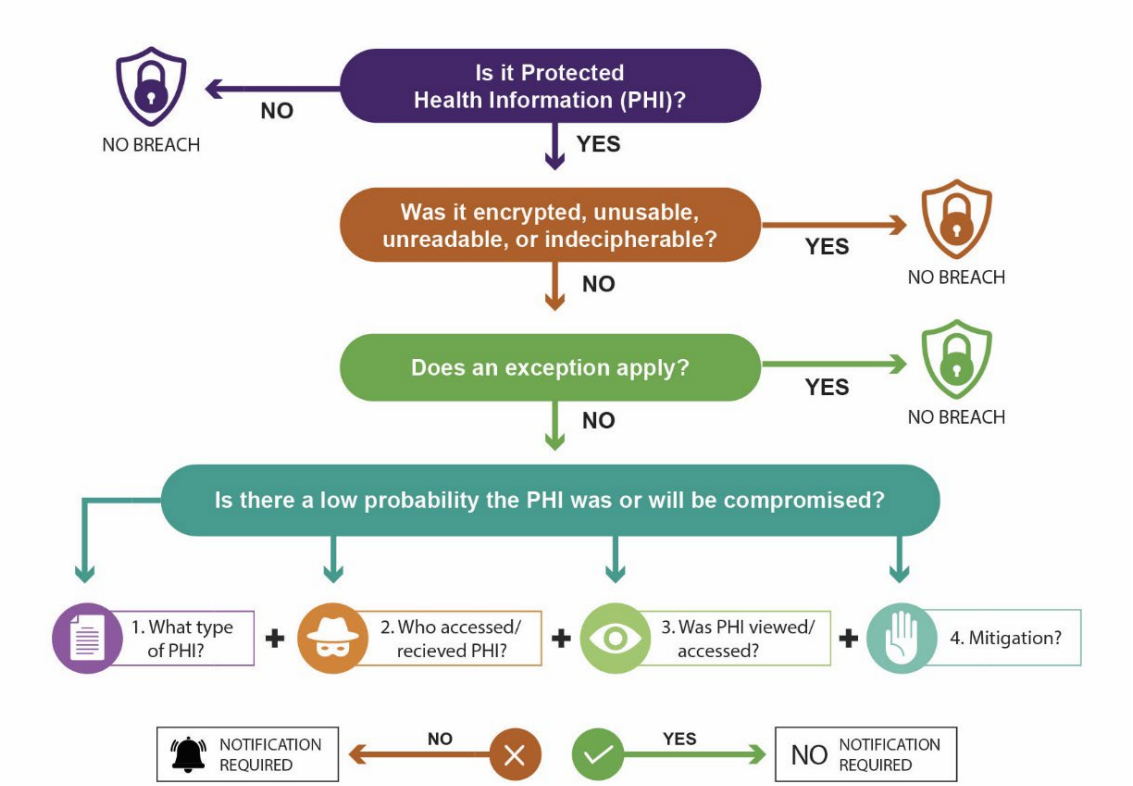
E. Practical Implementation of the HIPAA Breach Notification Policy and Procedures

Workforce members will report any disclosure of PHI that the workforce member believes may have been unauthorized or otherwise inappropriate and allow the HIPAA Privacy Officer to investigate and determine the next steps. Common HIPAA breaches include:

-  Emails containing PHI sent to the incorrect recipient;
-  Emails containing PHI forwarded to individuals who do not need access to the PHI for the purpose for which the PHI disclosure was authorized. For example, forwarding an email with PHI that was collected to secure insurance reimbursement to the HR department as a way to get an employee relations issue addressed is an unauthorized disclosure of PHI. Emails containing patient information should not be forwarded, even within the organization, unless the forwarded email is consistent with the use authorized by the patient (*e.g.,* to get Exogen reimbursed or to receive information from patient assistance);

- An unencrypted laptop containing PHI is stolen from a car or train;
- A ransomware attack of company systems results in the unauthorized encryption of electronic PHI rendering it at least temporarily inaccessible; and
- Lost "thumb drives" containing PHI.

F. HIPAA Breach Decision Flow



VI. HIPAA Privacy Officer Policy

A. HIPAA Privacy Officer Policy Statement

Bioventus will designate a HIPAA Privacy Officer whose general responsibilities are to:

- Oversee all HIPAA-related compliance activities, including the development, implementation, and maintenance of appropriate privacy policies and procedures;
- Conduct various risk analyses, as needed or when required by HIPAA;
- Serve as the point of contact for Bioventus HIPAA compliance related inquires;

- Manage HIPAA breach investigations, determinations, notifications, and responses; and
- Develop appropriate HIPAA training for all workforce members.

B. HIPAA Privacy Officer Procedures

Bioventus' HIPAA Privacy Officer is the Bioventus workforce member who must either perform the following functions or delegate the responsibility to a qualified workforce member:

- Develop and maintain specific policies and procedures mandated by HIPAA.
- Ensure compliance with HIPAA policies and consistent application of sanctions for failure to comply with such policies for all individuals in the organization's workforce, and for all Business Associates, in cooperation with Human Resources, IT, the executive team, and legal counsel, as applicable.
- Maintain an accurate inventory of (1) all roles that have access to PHI, and (2) all uses and disclosures of PHI by any role or entity.
- Administer patient rights requests.
- Administer the process for receiving, documenting, tracking, investigating, and acting on all complaints concerning Bioventus' HIPAA privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
- Cooperate with HHS and OCR, other legal entities, and organization officers in any compliance reviews or investigations.
- Work with the HIPAA Security Officer and appropriate technical personnel to (1) protect PHI from unauthorized use or disclosure, (2) oversee the HIPAA Security program, and (3) safeguard PHI through a HIPAA compliance plan with HIPAA Security standards, as required by the Security Rule.
- Draft, disseminate, and maintain the Privacy Notice(s) required by the HIPAA Privacy Rule, or designate an individual to do so.
- Determine when consent or authorization is required for uses or disclosures of PHI, and draft forms as necessary. See **Addendum H: HIPAA Authorization Form - Sample** for a sample HIPAA Authorization Form.
- Establish procedures for the review of contracts under which access to PHI is given to outside entities, bringing those contracts into compliance with the HIPAA Privacy Rule, and ensuring that confidential data is adequately protected when such access is granted.
- Ensure that all policies, procedures, and notices are flexible enough to respond to new technologies and legal requirements.
- Ensure that future initiatives are structured in such a way as to ensure patient privacy.
- Conduct periodic privacy assessments and take remedial action as necessary.
- Deter retaliation against individuals who seek to enforce their own privacy rights or those of others.
- Remain reasonably up-to-date and advise on new laws and technologies to protect data privacy, seek expert assistance where necessary, and update the policies and procedures periodically when changes in law or business processes affecting PHI occur.
- Evaluate and monitor data collected by or posted on Bioventus websites for compliance with applicable privacy laws and regulations.

VII. HIPAA and State Law Preemption Policy

A. Preemption Policy Statement

In addition to complying with HIPAA obligations, Bioventus will comply with state laws in the states where we operate. HIPAA generally preempts state laws regarding medical or health privacy. However, state laws that provide stronger protections than HIPAA for PHI or that provide additional patient and consumer access to health data can create additional obligations with which Bioventus must comply. HIPAA Covered Entities and Business Associates must follow both HIPAA and state law whenever possible. If there is a conflict between the two, a preemption analysis and determination should be made to assess which laws (HIPAA, state law, or both) to follow.

B. Preemption Procedures

- Bioventus' HIPAA Privacy Officer will assist in analyzing HIPAA preemption issues and making preemption determinations, with outside expert assistance, as necessary.
- The HIPAA Privacy Officer will assist in creating, modifying, or amending Bioventus' policies to accurately reflect the HIPAA Privacy Officer's preemption determinations and provide guidance to management on HIPAA and state law preemption issues, with outside expert assistance, as necessary.
- The HIPAA Privacy Officer will assist in monitoring legislative changes in the states where we operate that could affect HIPAA preemption issues, with outside expert assistance, as necessary.

C. Practical Implementation of State Preemption

Note that states like California whose laws acknowledge HIPAA preemption do so on a very narrow basis. State laws may provide higher standards of care, in which case, they are not preempted. They also carve out non-treatment related collection of PHI or personal information for things like marketing campaigns. Patients who visit online patient support portals or ask for information about a product on a webform are more likely to be covered by a state privacy law than HIPAA or maybe in addition to HIPAA. It is prudent to seek outside expert help if the HIPAA Privacy Officer is unsure whether an exemption or preemption applies.

VIII. HIPAA Training Policy

A. Training Policy Statement

Bioventus provides privacy and security HIPAA training to all members of its workforce who are likely to encounter IIHI or PHI during their work for Bioventus.

B. Training Procedures

- HIPAA training will be simple, easy to understand, and aligned to a person's role and their interactions with PHI, and will include a broad overview of HIPAA itself, the fundamentals of HIPAA's privacy and security requirements and restrictions, and a review of relevant and appropriate internal Policies related to HIPAA compliance.
- HIPAA training is provided to all new hires before they work with IIHI or PHI.

- HIPAA training and awareness is conducted at least once every year and completion is documented.
- HIPAA training includes measures to validate understanding, such as quizzes or games designed to measure the effectiveness of the training.
- The HIPAA Privacy Officer will coordinate with IT and develop and deploy HIPAA training and awareness materials to maintain a high level of HIPAA awareness among the workforce, with expert assistance, as necessary.

C. Practical Implementation of HIPAA Training

All workforce members will receive HIPAA training upon hire and annually. Additional, more specific, training will be provided to teams who handle a large volume of PHI, such as the Revenue Cycle and Patient Support Services teams. At a minimum, HIPAA training should emphasize that the entire workforce is responsible for HIPAA compliance, and should clearly define PHI, explain the Minimum Necessary Rule, and teach security awareness and good data practices, as well as how to respond to suspected HIPAA breaches.

IX. PHI Uses and Disclosures Policy and the Minimum Necessary Rule

A. Uses and Disclosures and Minimum Necessary Policy Statement

Bioventus conducts its operations in compliance with HIPAA's rules governing uses and disclosures of PHI.

- A use of PHI is the sharing, use, application, utilization, or examination of PHI by any workforce member.
- A disclosure is the release, transfer, or provision of access to, or divulgence of, PHI to persons who are not workforce members.
- There are no restrictions on disclosures of properly de-identified data, which is not covered by HIPAA.
- Bioventus follows the HIPAA Minimum Necessary Rule.
- Except where the Minimum Necessary Rule does not apply, workforce members will communicate only the minimum amount of PHI necessary to fulfil the purpose of the disclosure and avoid communicating PHI to individuals, including individuals within the Bioventus workforce, who do not need the PHI to facilitate patient treatment or reimbursement.
- When Bioventus is acting as a Covered Entity, it will disclose PHI only for treatment, payment healthcare operations, or when authorized by the patient or patient's lawful representative.
- When Bioventus is acting as a Business Associate, it will use and disclose PHI only as permitted and prescribed in the BAA.

B. Uses and Disclosures and Minimum Necessary Procedures

- **Minimum Necessary**. When using or disclosing PHI, or when requesting PHI from another Covered Entity or Business Associate, workforce members must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
    - This means that PHI will not be included in emails sent to workforce members not tasked with completing Exogen orders, patient assistance, or another specifically authorized task where PHI is required for legitimate and tailored purposes.

- Before sharing PHI ask yourself whether the individual receiving it needs it to complete a task.
- Never share more PHI than is needed to complete a task.
- Remember that HIPAA Authorization is not organization wide. Workforce members will not share PHI with other workforce members unless those individuals need the information for authorized purposes.

! If a workforce member receives an email or other message with PHI that the receiving workforce member does not need to fill an Exogen order, or for another lawful reason (such as to respond to a subpoena or pursuant to a BAA), that workforce member will delete the email completely and notify the sender (using a new email chain) that the disclosure did not comply with these Policies, with a cc: to the HIPAA Privacy Officer. The HIPAA Privacy Officer will determine whether re-training is required in response to the incident.

- **Exceptions to Minimum Necessary**. The minimum necessary standard applies in most situations, with some important exceptions where it does not apply. The minimum necessary standard does not apply to:
  - Disclosures to a health care provider for treatment purposes (including disclosures specified under a hospital agreement);
  - Disclosures to the individual who is the subject of the information (including in response to access, amendment, or accounting requests);
  - Uses or disclosures made pursuant to a valid HIPAA Authorization;
  - Disclosures to the Secretary of the US Department of Health and Human Services to determine Bioventus' compliance with the HIPAA Privacy Rule;
  - Uses or disclosures that are required by law; and
  - Uses or disclosures that are required for compliance with HIPAA.
- **Deceased Patient Disclosures**. When operating as a Covered Entity, Bioventus will only disclose PHI subject to the minimum necessary rule. When operating as a Business Associate, Bioventus will only disclose PHI as permitted and prescribed in the BAA.
- **PHI Disclosure Table**. See **Addendum E: PHI Disclosure Table** for a PHI Disclosure Table defining common scenarios for acceptable disclosures of PHI, including different types of requestors and whether authorization is required and a copy fee should be charged.
- **Capturing Patient Documentation**. Patient information may be captured using company issued scanners, physician scanners, or fax machines, including e-fax. Workforce members will not use mobile devices to take photographs of patient records and text or email to colleagues because such photographs may be inappropriately saved to services such as iCloud.
- **Photographs**. Photographs required to fit patients for devices or taken during surgical procedures should avoid, where at all possible, capturing patient faces or other identifying features such as tattoos. Photographs must be taken on company issued or BYOD devices with mobile device management software installed and transmitted in a manner consistent with these Policies and immediately deleted from the device's photo library after transmission. When in doubt, contact the HIPAA Privacy Officer prior to taking a photo.
- **Especially Sensitive Information**. For especially sensitive information, such as diagnosis of STIs like AIDS/HIV, and mental health issues, alcohol and drug abuse prevention and treatment, and the like, patient consent to disclosure must be informed (*i.e.,* made with the patient's or consumer's knowledge of the risks and benefits of disclosing the specific sensitive information).
- **Use & Disclosures of PHI**. Bioventus will use and disclose PHI consistent with these Policies and applicable BAAs.

- Bioventus may disclose PHI without a patient authorization for treatment, payment, and health care operations purposes, as those terms are defined under HIPAA.
- Bioventus may also use or disclose PHI without authorization for public policy purposes including:
  - Investigations into abuse, neglect, or domestic violence;
  - For judicial proceedings;
  - For law enforcement purposes;
  - For public health activities;
  - For health oversight activities;
  - About decedents;
  - For limited research purposes, as described in these Policies;
  - To avert a serious threat to health or safety; and
  - For worker compensation purposes.
- All other uses or disclosures require individual authorization

- **Social Media and Text**. PHI should never be disclosed via social media, SMS text, or instant messaging applications.
- **Costs**. Bioventus incurs costs when releasing patient information (copying, postage, and so forth) and is permitted under HIPAA regulations and state law to charge a reasonable fee to offset those costs. To the extent practicable, the following priorities and time frames will apply to requests for disclosures of PHI:
  - Emergency requests involving immediate emergency care of patient:
    - Immediate processing.
  - Priority requests pertaining to the current care of a patient:
    - Within one workday.
  - Patient request for access to their own record:
    - Within three workdays.
  - Subpoenas and depositions:
    - As required.
  - All other requests:
    - Within five workdays.
- **Courtesy Notifications to Practitioners**. As a courtesy, records processing personnel will notify the appropriate healthcare practitioner when any of the following occur:
  - Patient or their representative requests information from the medical record;
  - Patient or representative requests direct access to the complete medical record; or
  - Patient or representative institutes legal action.
- **Disclosure Monitoring and Logging**. The HIPAA Privacy Officer, or their designee, will maintain a log to track non-routine requests for the release of PHI. The log will contain the following information:
  - Date Bioventus received the request;
  - Name of patient;
  - Name and status (patient, parent, guardian) of the person making the request;
  - Information released;
  - Date released; and
  - Fee charged.
- **Fee Schedule**. Bioventus will process requests for information from patient records in a timely, consistent manner as set forth in these Policies.
  - Bioventus may charge a reasonable fee to offset the costs associated with specific categories of requests. The HIPAA Privacy Officer, or their designee, will develop and

implement a Fee Schedule related to disclosures of PHI. Fees will be based on an assessment of such factors as the costs of equipment and supplies, employee costs, and administrative overhead and will include postage (including express mail or courier costs) when incurred at the request of the authorizing party. For requests for records in electronic format, HIPAA permits fees to include only direct labor costs when responding to such requests. Individual states have also established maximum fees for copies of patient records.

- Unless the request specifies release of the complete medical record, Bioventus will only release selected portions of the record accompanied by a cover letter detailing the items included.

- **Disclosure Quality Control**. The HIPAA Privacy Officer will conduct a periodic review of the release of information, as needed, paying attention to the following:
  - Validity of authorizations;
  - Appropriateness of information abstracted in response to the request;
  - Retention of authorization, request, and transmitting cover letter;
  - Procedures for telephone, electronic, and in-person requests;
  - Compliance with designated priorities and time frames;
  - Proper processing of fees; and
  - Maintenance of confidentiality.

C. Practical Implementation of Uses and Disclosures and Minimum Necessary

Workforce members should always ask themselves two questions before sharing PHI:

- (1) Who is authorized to see this information because they need it for the purpose for which Bioventus collected the information?
  - For example, to process payment for an order.
- (2) How much PHI is necessary to achieve this purpose?
  - It is never appropriate to review the PHI of family members or friends, even if your intent is simply to speed up their order process.
- Where possible, PHI used in the Exogen order process should be maintained and shared in Exogen Direct rather than by email. In cases where it must be transmitted by email every measure should be taken to ensure:
  - The email is sent to the correct recipient;
  - PHI is in password protected attachments, where possible; and
  - PHI is limited to what is necessary.
- Workforce members will avoid receiving PHI that Bioventus does not reasonably need in its role as either a Covered Entity or a Business Associate by instructing healthcare providers, Business Associates, and other PHI providers to provide Bioventus only what is reasonably necessary.

X. Transmission of PHI

A. Transmission of PHI Policy

During the transmission of PHI, Bioventus workforce members will properly safeguard the information to avoid unauthorized disclosure. This Policy establishes the permissible transmission methods.

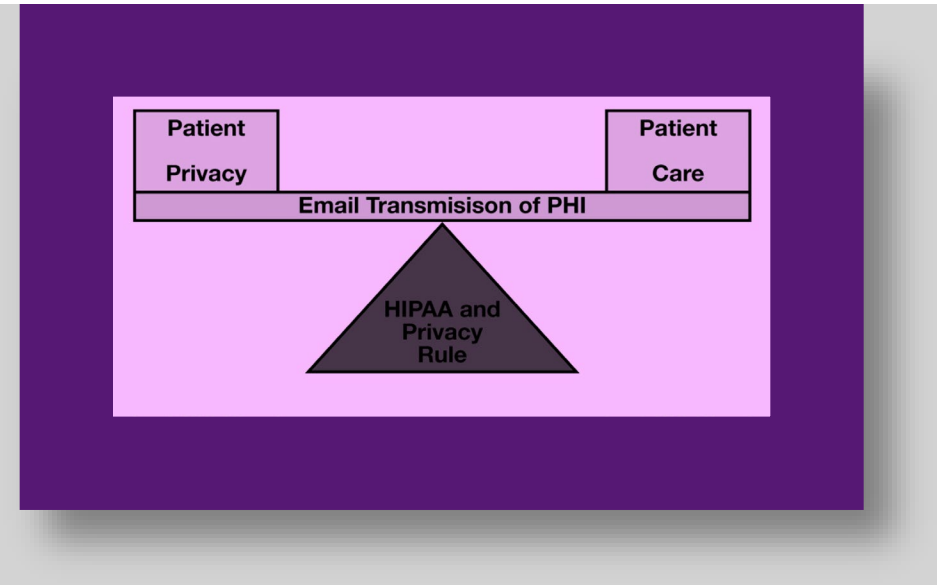
B. Transmission of PHI Procedures

- **Email**. When sending or receiving PHI via email and email attachments, workforce members will make reasonable attempts to ensure that the email message and any attachments are not read or accessed by individuals who are not authorized to access the PHI, and to send PHI through encrypted emails, which can be done automatically or manually. Workforce members will use reasonable efforts to confirm the identity of individuals receiving PHI via email. Emails should contain only the minimum of amount of PHI necessary to achieve the purpose of the communication and should be avoided if more secure methods of communication are available. Emails sent outside the organization containing PHI must contain the following statement in the email footer:
  - *"This email contains Protected Health Information concerning a patient and is protected by applicable law, including the Health Insurance Portability and Accountability Act (HIPAA). This email and any attachments are confidential. This information is intended only for the use of the individuals or entities intended as recipients. If you are not the intended recipient, you are hereby notified that any collection, use, disclosure, copying, distribution of, or action taken in reliance on the contents of these documents is strictly prohibited. The intended recipient is required to maintain this information in a secure and confidential manner and is prohibited from re-disclosing it without first obtaining the patient's consent or as otherwise permitted by law. If you prefer not to receive such patient information via email, or if you believe you have received this email in error, please notify us immediately by email at privacy@bioventus.com. Thank you."*
- **Fax or eFax**. PHI may be transmitted by secure facsimile, including eFax.
- **Telephone**. When transmitting PHI by telephone, workforce members will make reasonable efforts to uphold a high level of discretion and be mindful of their surroundings and the ability of others to overhear their conversation. Workforce members should make reasonable efforts to validate the identity of the individual with whom they are discussing PHI.
- **Internet Download or Data Transfer**. Bioventus will take reasonable steps to ensure internet data transfer involving IIHI or PHI are conducted securely and otherwise in conformance with these Policies. Workforce members should coordinate with the HIPAA Privacy Officer or the VP of Global Information Systems to ensure that internet transfer protocols are secure prior to using a new method to transmit PHI over the internet.
- **Exogen Direct**. Exogen Direct is the preferred method for transmitting PHI within Bioventus. PHI may be uploaded into Exogen Direct and communications can then include a link to the system. This helps Bioventus maintain PHI in a centralized, secure system, and limits the need to include PHI in the bodies of emails.

C. Practical Implementation of Transmission of PHI

Bioventus must always balance patient privacy and patient care. Email is particularly challenging because of the accidental misdirection of emails and the forwarding of emails that a sender may not realize has PHI in a message further down in a thread. For this reason, Bioventus strongly prefers the use of Exogen

Direct for internal communications containing PHI. When email is used, it must be used carefully and deliberately.



XI. Incidental Disclosures of PHI

A. Policy Regarding Incidental Disclosure

Bioventus will implement reasonable administrative, technical, and physical safeguards to limit incidental uses or disclosures of PHI. However, an incidental disclosure does not violate these Policies if reasonable measures are taken to prevent such disclosure and the disclosure resulted from a use or disclosure that is otherwise permissible under these Policies and HIPAA. An incidental disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and occurs due to a disclosure permitted by HIPAA.

B. Procedures Regarding Incidental Disclosure

An incidental disclosure is a disclosure of PHI that occurs as a by-product of permissible uses or disclosures. Examples include leaving PHI on a public surface, someone seeing PHI while "shoulder surfing" a screen containing PHI used by an authorized employee, or someone overhearing a verbal discussion of PHI.

Workforce members will avoid incidental disclosures where possible by making sure to:

- Comply with Policies related to the transmission of PHI;
- Speak quietly when discussing PHI in any non-private area;
- Log out of computers when stepping away from a workstation that can be used to access PHI and comply with all IT Security procedures; and
- Maintain a clean desk, locking away PHI when you are not at your desk, and ensure PHI is not left on printers and faxes wherever possible.

XII. Use and Disclosure of PHI for Research Purposes

A. Use and Disclosure for Research Purposes Policy

Bioventus will obtain authorization from an individual patient where it is required under applicable law to conduct research involving PHI. Bioventus may use or disclose PHI for research purposes without patient authorization in certain situations outlined in these Policies.

B. Research Disclosure Procedures

All research activities must be reviewed and approved by the Bioventus R&D team in accordance with applicable R&D policies and procedures.

- **Waiver of Authorization**. Bioventus may use or disclose PHI for research without authorization if either an IRB or a Privacy Board approves a waiver of the authorization. The IRB or Privacy Board must be established according to applicable law. Documentation of the IRB or Privacy Board approval must be provided to the HIPAA Privacy Officer who will review it and determine if the disclosure can be made.
- **Reviews in Preparation for Research**. Bioventus may allow a researcher employed by a Covered Entity (such as a hospital) to review PHI in preparation for research. The researcher must first provide to the HIPAA Privacy Officer, or a designated representative, a written statement that:
    - The use or disclosure is sought solely to review PHI as needed to prepare a research protocol (or for a similar purpose in preparation for research);
    - No PHI will be removed from Bioventus by the researcher in the course of the review; and
    - The PHI sought is necessary for the research purposes.
- **Research on Decedents' Information**. PHI concerning a deceased individual may be used or disclosed to a Covered Entity (such as a hospital) for research purposes. The researcher must first provide to the Privacy Officer, or a designated representative, a written statement that:
    - A representation that the use or disclosure sought is solely for research on the PHI of decedents;
    - Documentation, at the request of Bioventus, of the death of such individuals; and
    - A representation that the PHI for which use or disclosure is sought is necessary for research purposes.

XIII. Use and Disclosure of PHI in Limited Data Sets

A. Policy on Use and Disclosure in Limited Data Sets

Bioventus may disclose a limited data set of PHI to an outside party who is not party to a BAA without a patient's authorization only for lawful research, public health purposes, or health care operations purposes, provided the recipient has signed a Data Use Agreement. See **Addendum F: Sample Data Use Agreement - Annotated** for a sample Data Use Agreement.

Where Bioventus maintains PHI for research or treatment purposes, it may create and use a limited data set for research or public health purposes pursuant to a Data Use Agreement.

B. Procedures for Use and Disclosure in Limited Data Sets

- A limited data set is information from which the following identifiers have been removed:
    - Names;

- Street addresses (other than town, city, state, and zip code);
- Telephone numbers;
- Fax numbers;
- Email addresses;
- Social Security numbers;
- Medical records numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate license numbers;
- Vehicle identifiers and serial numbers, including license plates;
- Device identifiers and serial numbers;
- URLs;
- IP address numbers;
- Biometric identifiers (including finger and voice prints); and
- Full face photos (or comparable images).

- A limited data set may include:
  - Dates of admission, discharge, service, DOB, and DOD;
  - City, state, and five-digit zip code; and
  - Age in years, months, days, and hours.
- **Third-party requests**. All third-party requests for limited data sets must be documented in writing and reported to the HIPAA Privacy Officer, who shall approve all third-party requests for a limited data set. A request for a limited data set must include the following:
  - Requestor's name, address, telephone numbers, title, and organization;
  - Date of request;
  - Purpose of the request (*e.g.,* research, public health, or health care operations), including the intended uses, any re-disclosures, and who will use or have access to the limited data set;
  - Names of all recipients of the limited data set;
  - Nature of information requested (*e.g.,* time period, minimum number of patient records, type of patient records); and
  - Date the limited data set is needed.
- **Data Use Agreements**. Bioventus must execute a Data Use Agreement with recipients of a limited data set. A request for a limited data set will be denied if the recipient refuses to execute a Data Use Agreement. This requirement will not apply, however, to the extent the limited data set recipient is a Business Associate that is already permitted to receive PHI under a BAA. The Data Use Agreement must:
  - Establish the permitted uses and disclosures of the limited data set;
  - Identify who may use or receive the information;
  - Prohibit the recipient from using or further disclosing the information, except as permitted by the agreement or as permitted by law;
  - Require the recipient to use appropriate safeguards to prevent a use or disclosure that is not permitted by the agreement;
  - Require the recipient to report to the Covered Entity any unauthorized use or disclosure of which it becomes aware;
  - Require the recipient to ensure that any agents (including a subcontractor) to whom it provides the information will agree to the same restrictions as provided in the agreement; and
  - Prohibit the recipient from identifying the information or contacting the individuals.

XIV. Sale of PHI

A. Sale of PHI Policy

As a rule, Bioventus does not sell PHI. If an exception to this Policy is made pursuant to the procedure set forth below, Bioventus will obtain an informed patient authorization for any disclosure that constitutes a sale of PHI for direct or indirect remuneration, to the extent permitted by any BAA or law. Any such authorization must state that the disclosure will result in remuneration to Bioventus, if applicable.

B. Procedures for Exceptions to the Prohibition on Sale

If a workforce member proposes a business case involving the sale of PHI, the workforce member must contact the HIPAA Privacy Officer as soon as the proposed business case is developed and before any PHI is sold or contracted for sale. Except as described below, a written prior authorization is required for a sale of PHI, and PHI may not be sold without the prior express approval of the HIPAA Privacy Officer.

- An authorization is generally not required for the sale of PHI in the following instances:
  - For public health activities as described in the HIPAA Privacy Rule;
  - In connection with research (provided the price is a reasonable, cost-based fee to cover the cost to prepare and transmit the data for such research);
  - For treatment of the individual;
  - In connection with a BAA; or
  - To provide an individual with a copy of their own records.

XV. Authorization and Capacity to Authorize

A. Policy on Capacity to Authorize

Bioventus requires signed, current, and valid patient authorization to release PHI as set forth in the procedures below.

B. Procedures on Authorization

Bioventus requires a written, signed, current, valid authorization to release medical information as follows:

Patient Category	**Required Signature**
Adult patient	The patient or a duly authorized representative, such as a court-appointed guardian or attorney. Proof of authorized representation required (such as a notarized power of attorney).
Deceased patient	Next of kin as stated on admission face sheet (state relationship on authorization) or executor/administrator of the estate.
Unemancipated minor	Parent, next of kin, or legally appointed guardian or attorney (proof of relationship required).

Emancipated minor	Same as adult patients above.
Psychiatric, drug, or alcohol program patients/clients	Same as adult patients above but check for special requirements.
AIDS/HIV or other STI patients	Same as adult patients above but check for special requirements.

- **Authorization Forms**. The HIPAA Privacy Officer will develop and use an approved authorization form. All personnel will use this form whenever possible. All personnel will, however, honor letters and other forms, provided they include all the required HIPAA information.
- **Authorization**. A Covered Entity may not use or disclose PHI without a valid HIPAA Authorization, except that no authorization is required to carry out patient heath care treatment, for payment for such treatment, or for healthcare operations. Patients must be provided with a copy of any executed authorizations. To be valid, a HIPAA Authorization must be written in plain language and contain:
    - A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
    - The name or other specific identification of the person or class of persons authorized to make the use or disclosure;
    - A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement as to the purpose;
    - An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statements "end of the research study" or "none" or similar language is sufficient if the use or disclosure of PHI is for research; and
    - Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.
- **Revocation of Authorization**. A patient may revoke an authorization by providing a written statement to Bioventus. The revocation will become effective when we receive it but will not apply to disclosures already made. The authorization must set forth the right of revocation and the method for invoking it.
- **Refusal to Honor Authorization**. The HIPAA Privacy Officer, or others authorized to release information, will not honor a patient authorization when they have a reasonable doubt or question as to the following information:
    - Identity of the person presenting the authorization;
    - Status of the individual as the duly appointed representative of a minor, deceased, or incompetent person;
    - Legal age of, or status as, an emancipated minor;
    - Patient's capacity to understand the meaning of the authorization;
    - Authenticity of the patient's signature; or
    - Current validity of the authorization.

In such situations, the employee will refer the matter to the HIPAA Privacy Officer for review and decision.

- See **Addendum D: Person and Identity Verification Table** for a Person and Identity Verification Table for how to verify a person's identity during an in-person encounter, a telephone encounter, and/or a request in writing (fax, mail, hand-delivered).
- See **Addendum E: PHI Disclosure Table** for a table defining common scenarios for acceptable disclosures of PHI, including different types of requestors and whether authorization is required and a copy fee should be charged.

XVI. HIPAA Patient Rights Policy

A. Patient Rights Policy Statement

Bioventus honors lawful patient rights requests pursuant to HIPAA or other applicable state or federal laws. Bioventus does not retaliate against individuals asserting HIPAA or other legally protected rights.

B. Patient Rights Procedures

The VP of Patient Access and Reimbursement coordinates Bioventus' response to patient access requests. Patient information relevant to patient rights requests includes only that information contained in each patient's Designated Record Set (**"DRS"**), which is defined as:

- **Designated Record Set**. A group of records maintained by or for a Covered Entity that is:
  - The medical and billing records about individuals maintained by or for a covered health care provider;
  - The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; and
  - Used, in whole or in part, by or for the Covered Entity to make decisions about individuals.
- **Record**. The term "record" means any item, collection, or grouping of information that includes Protected Health Information (**"PHI"**) and is maintained, collected, used, or disseminated by or for a Covered Entity.
- **Rights**. Bioventus provides the patient rights that are required by HIPAA, including:
  - The right to receive a copy of HIPAA Notice of Privacy Practices, which details how Individually Identifiable Health Information (**"IIHI"**) may be used or disclosed by Bioventus;
  - The right to review or obtain a copy of medical records about that patient, or about the patient's minor children;
  - The right to request that Bioventus restrict the use or disclosure of the patient's medical records;
  - The right to receive IIHI at an alternate address or through alternate delivery means, such as by fax or courier;
  - The right to request amendments to medical records, which Bioventus then passes on to the patient's medical provider;
  - The right to an accounting of certain disclosures of IIHI; and
  - The right to file a privacy complaint directly with Bioventus, or with the federal government.

XVII. HIPAA Privacy Complaints Policy

A. Complaints Policy Statement

- Bioventus prohibits non-professional or retaliatory acts against any person or patient who files a privacy complaint or exercises any right guaranteed under HIPAA.
- Bioventus timely responds to all complaints submitted by any person, party, patient, or workforce member.
- The HIPAA Privacy Officer, or their designee, is responsible for the acceptance of, management of, and response to complaints, and will establish a process to receive, document, and process complaints.

B. Complaints Procedures

- All complaints must be submitted in writing, dated, and signed by the complainant.
- Bioventus will investigate and respond to all complaints with a written response within 30 days of the time each complaint is submitted. If more time is required to investigate and resolve a specific complaint, the complainant will be notified in writing that additional time is required to investigate and resolve the complaint within 30 days after each complaint is submitted. In no case will more than 60 days elapse between the time a complaint is submitted and the time the complaint is resolved.
- The HIPAA Privacy Officer, or their designee, will investigate each complaint in a fair, impartial, and unbiased manner. Parties named in the complaint, or who participated in events leading to the complaint, will be interviewed in a professional and non-coercive manner.
- The final resolution or disposition of each complaint will be documented, pertinent portions provided to the complainant, and retained in accordance with Bioventus' HIPAA Documentation Retention Policy.
- In addition to providing complainants with a written response to their complaint, meritorious complaints will be resolved with remediation appropriate to the severity of the situation. Such remediation may include, but is not limited to:
    - A written apology to the complainant from Bioventus;
    - In the event of a HIPAA breach involving the complainant's PHI, credit-monitoring service for the complainant for a period of one or two years, paid for by Bioventus;
    - Financial compensation, if determined to be appropriate by legal counsel or senior management;
    - Sanctions against workforce members, as appropriate to the circumstances; or
    - Other unspecified remediation(s), as determined by legal counsel and senior management.

XVIII. HIPAA Risk Management Process Policy

A. Risk Management Policy Statement

- Bioventus will establish, implement, and maintain an appropriate risk management plan which will be under the control and supervision of the HIPAA Privacy Officer.
- Business and IT "best practices," along with the research and recommendations of the National Institute for Standards and Technology (**"NIST"**), will be included in the development and execution of the risk management plan.

- The Bioventus risk management plan will make every effort to identify, analyze, prioritize, and minimize identified risks to the privacy, security, integrity, and availability of PHI. The nature and severity of various risk and risk elements will be identified, with the goal of reducing risk as much as is reasonably practicable. Risk management will be updated, analyzed, and improved on a continuous basis.
- The results of the risk management process will be input into management's decision-making processes to help reduce our overall risk and to comply with HIPAA.
- The Bioventus Board of Directors will be informed periodically of HIPAA risk management, analyses, and mitigation.

B. Risk Management Procedure

- Bioventus HIPAA risk management is ongoing with risk mitigation measures undertaken as necessary, reviewed, and re-evaluated periodically as set forth the HIPAA Risk Analysis and HIPAA Risk Management Policies and related IT policies and procedures.
- The HIPAA Privacy Officer will lead the HIPAA Risk Management Team, which includes:
    - General Counsel;
    - Director, Internal Audit;
    - VP of Global Information Systems; and
    - VP Patient Access & Reimbursement.
- The HIPAA Privacy Officer will present a proposed risk management plan for approval by the HIPAA Risk Management Team.
- HIPAA risks will be measured according to Bioventus' Enterprise Risk Management impact and likelihood criteria. HIPAA risks that remain "High" after compensating controls are put in place will be accepted, or not, by the Bioventus Board of Directors.

C. Risk Management Policy Implementation

Measures required to implement this Policy are set forth in the HIPAA Risk Analysis and HIPAA Risk Management Policies and in **Addendum G: HIPAA Risk Assessment Analysis and Methodology per OCR Guidance**.

XIX. HIPAA Risk Analysis Policy

D. Risk Analysis Policy Statement

- Bioventus will conduct periodic assessments of potential risks and vulnerabilities to the confidentiality, integrity, and availability of the PHI with which it is entrusted.
- The HIPAA Privacy Officer is responsible for leading the HIPAA Risk Management Team in conducting periodic risk analyses, will establish a plan and procedures for such analyses, and ensure such analyses are properly documented and maintained.

E. Risk Analysis Procedures

These procedures will be read in coordination with Bioventus' IT Security and Information Systems policies and procedures.

- HIPAA risk analyses and assessments will be conducted periodically, as new or changed processes are implemented, and the entire HIPAA privacy and security program will be assessed internally

at least annually. The Bioventus HIPAA privacy and security program will be assessed by an expert third party at least every 2 years.

- The HIPAA risk analysis process will be modeled upon the risk analysis process recommended by NIST, specifically NIST 800-53 and NIST SP 800-66 Rev.2 (or more current revisions). See **Addendum G: HIPAA Risk Assessment Analysis and Methodology per OCR Guidance** for risk analyses guidance.
- Risk analysis will be conducted throughout the IT system life cycles:
    - Before the purchase or integration of new technologies involving PHI;
    - When integrating new technologies into systems containing PHI; and
    - While sustaining and monitoring appropriate security controls.
- Scoring of risks will be in accordance with the Bioventus Enterprise Risk Management definitions and methodology.
- As discussed in further detail in the HIPAA Risk Management Policy, risk mitigation is a process that prioritizes, evaluates, and implements security controls that will reduce, or offset risks identified during the risk analysis.
- Identified HIPAA risks will be assigned a risk owner, who is responsible for implementing recommended HIPAA risk mitigation controls.
- The results of risk analyses and assessments will become an integral part of management's decision-making process and will guide decisions related to the protection of PHI.
- All such risk analyses and assessments will be documented in accordance with Bioventus' HIPAA Documentation Retention Policy and HIPAA Regulations.

F. Implementation of Risk Analyses

Bioventus will train workforce members of the need for risk analyses to be performed when systems containing PHI are implemented, integrated, or otherwise modified. Specific training will be provided to procurement, IT, and legal workforce members who are likely to be made aware in the early stages of planned projects that could impact the confidentiality, integrity, and availability of PHI. The HIPAA Privacy Officer must maintain copies of all documents related to risk analyses. These are often requested when HHS investigates a HIPAA breach or other complaint.

XX. HIPAA Risk Management Implementation Policy

A. Risk Management Implementation Policy Statement

- The HIPAA Privacy Officer and the HIPAA Risk Management Team are responsible for the implementation of the HIPAA privacy and security Risk Management Process.
- The Bioventus HIPAA Risk Management Team is tasked with planning and executing Bioventus' HIPAA Risk Management Implementation Policy and for identifying risks and complaints and documenting remediation plans for mitigating material HIPAA risks identified during risk analyses and assessments.

B. Risk Management Implementation Procedure

- This HIPAA Risk Management Implementation Policy and its procedures are integral to Bioventus's other risk management efforts, including the Bioventus HIPAA Risk Management Process Policy and HIPAA Risk Analysis Policy.

- All identified HIPAA risks will have an identified risk owner, who is accountable for implementing mitigating controls.
- The Bioventus Board of Directors is responsible for accepting, or not, all HIPAA risks that remain High after mitigation efforts are complete.

C. Practical Implementation of Risk Management

- OCR has issued guidance on HIPAA risk assessments under the Security Rule, which can be found here:
  - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
  - A summary of the OCR guidance is set forth in **Addendum G: HIPAA Risk Assessment Analysis and Methodology per OCR Guidance**.
- HealthIT.gov maintains a simple security risk assessment tool to help Bioventus comply with administrative, technical, and physical safeguards. The security risk assessment tool is available for download here:
  - https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

XXI. HIPAA Sanctions Policy

A. Sanctions Policy Statement

- Bioventus will implement fair and appropriate sanctions for workforce members who fail to follow these HIPAA Policies.
- Sanctions will be appropriate to the nature and severity of the error or offense, and will consist of an escalating scale of sanctions, with less severe sanctions applied to less severe errors and offenses, and more severe sanctions applied to more severe errors and offenses.
- Certain offenses relating to IIHI or PHI can result in immediate termination, including, but not limited to:
  - Theft or intentional misappropriation;
  - Intentional lying or deception; or
  - Drug or alcohol use while handling PHI.
- Offenses involving obvious illegal activity may result in notifications to appropriate law enforcement authorities.
- Bioventus fully documents all workforce sanctions and their dispositions, according to our HIPAA Documentation Retention Policy and HIPAA requirements.

XXII. Business Associates Policy

A. Business Associates Policy Statement

Bioventus establishes and maintains business and working relationships with Business Associates in compliance with HIPAA requirements as required by law.

- HIPAA specifically identifies the following types of entities as Business Associates:
    - Subcontractors;
    - Patient safety organizations;
    - Health Information Organizations (**"HIOs"**), which include Health Information Exchanges (**"HIEs"**) and regional health information organizations;
    - E-prescribing gateways;
    - Personal Health Record (**"PHR"**) vendors that provide services on behalf of a Covered Entity; and
    - Other firms or persons who "facilitate data transmission" that requires routine access to PHI.
- The "**Minimum Necessary Rule**" applies directly to Business Associates and their subcontractors. When using, disclosing, or requesting PHI, these entities must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
- Business Associates' subcontractors are treated as Business Associates themselves. A subcontractor is defined as a person or entity to whom a Business Associate delegates a function, activity, or service involving PHI, but is not a member of the Business Associate's own workforce.
- Bioventus is not required to enter into a contract or other arrangement with a Business Associates' subcontractors; that is the responsibility of the Business Associate.

B. Business Associates Procedures

The HIPAA Privacy Officer is the Bioventus workforce member who must either perform the following functions or delegate the responsibility to a qualified workforce member:

- Maintain appropriate and lawful relationships with Business Associates;
- Ensure that Business Associate contracts meet HIPAA requirements and standards;
- Document all Business Associate related contracts and activities, in accordance with our HIPAA Documentation Retention Policy and HIPAA requirements;
- Ensure that IIHI and PHI are properly protected and safeguarded by our Business Associates; and
- Ensure that Business Associates:
    - Understand the importance and necessity of protecting IIHI and PHI, whether in electronic or hardcopy form;
    - Have proper and appropriate safeguards in place for IIHI and PHI before entrusting such information to them; and
    - Understand and are properly prepared to detect and respond to breaches of IIHI and PHI.

XXIII. Addenda

A. **Addendum A**: **HHS list of items and people that may be requested, examined, or interviewed during an investigation**

Workforce personnel that may be interviewed:

- President, CEO, or Director;
- HIPAA Privacy, Security, or Compliance Officers;
- Lead Systems Manager or Director;
- Systems Security Officer;
- Lead Network Engineer and/or individuals responsible for:
    - Administration of systems which store, transmit, or access PHI;
    - Administration systems networks (wired and wireless);
    - Monitoring of systems which store, transmit, or access PHI; or
    - Monitoring systems networks;
- Computer Hardware Specialist;
- Disaster Recovery Specialist or person in charge of data backup;
- Facility Access Control Coordinator (physical security);
- HR Representative;
- Director of Training; and
- Incident Response Team Leader.

Documents and other information that may be requested for investigations/reviews:

Policies, procedures, and other evidence that address the following:

- Prevention, detection, containment, and correction of security violations.
- Employee background checks and confidentiality agreements.
- Establishing user access for new and existing employees.
- List of authentication methods used to identify users authorized to access PHI.
- List of individuals and contractors with access to PHI to include copies of pertinent Business Associate Agreements (**"BAAs"**).
- List of software used to manage and control access to the internet.
- Detecting, reporting, and responding to security incidents.
- Physical security.
- Encryption and decryption of PHI.
- Mechanisms to ensure integrity of data during transmission, including portable media transmission (*i.e.,* laptops, cell phones, blackberries, thumb drives).
- Monitoring systems use - authorized and unauthorized.
- Use of wireless networks.
- Granting, approving, and monitoring systems access (*e.g.,* by level, role, and job function).
- Sanctions for workforce members in violation of policies and procedures governing PHI access or use.
- Termination of systems access.
- Session termination policies and procedures for inactive computer systems.
- Policies and procedures for emergency access to electronic information systems.
- Password management policies and procedures.

- Secure workstation use, including documentation of specific guidelines for each class of workstation (*i.e.,* on site, laptop, and home system usage).
- Disposal of media and devices containing PHI.

Other Documents:

- Entity-wide Security Plan.
- Risk Analysis (most recent).
- Risk Management Plan (addressing risks identified in the Risk Analysis).
- Security violation monitoring reports.
- Vulnerability scanning plans, including results from the most recent vulnerability scan.
- Network penetration testing policy and procedure, including results from the most recent network penetration test.
- List of all user accounts with access to systems which store, transmit, or access PHI (for active and terminated employees).
- Configuration standards to include patch management for systems which store, transmit, or access PHI, including workstations.
- Encryption or equivalent measures implemented on systems that store, transmit, or access PHI.
- Organization chart to include staff members responsible for general HIPAA compliance to include the protection of PHI.
- Examples of training courses or communications delivered to staff members to ensure awareness and understanding of PHI policies and procedures (security awareness training).
- Policies and procedures governing the use of virus protection software.
- Data backup procedures.
- Disaster recovery plan.
- Disaster recovery test plans and results.
- Analysis of information systems, applications, and data groups according to their criticality and sensitivity.
- Inventory of all information systems to include network diagrams listing hardware and software used to store, transmit, or maintain PHI.
- List of all Primary Domain Controllers (**"PDCs"**) and servers.
- Inventory log recording the owner and movement media and devices that contain PHI.

B. Addendum B: Model HIPAA Breach Notification Letter Template from the American Health Information Management Association

Letterhead Recommended
(Includes organization's full name and address)

[Date]

[Victim or Representative Name]
[Address Line 1]
[Address Line 2]
[City, State Zip Code]

Re: Personal *[Health]* Information of *[Name of Victim]*

Dear [Addressee Name -- Victim or Representative]:

On *[date], [name of responsible healthcare organization]* became aware of a breach of *[your/loved one's]* personal health information. We *[have identified/estimate]* the date of information leakage to be *[date]. OR [The duration of information exposure was (include date range and time range)].* OR [*We are unable to determine the date of the breach occurrence.]* We are notifying affected individuals in as timely a manner as possible so you can take swift personal action along with our organization's efforts to reduce or eliminate potential harm. *[It was necessary to delay notification because of the protected nature of the forensic investigation.]* Incident investigation *[is/is not]* complete at this time.[2]

The incident[3] involving protected health information was *[loss/theft/other] [state the circumstances]. [Examples: theft of a laptop containing files of 5,326 individuals from the trunk of a car* OR *exposure of personal health information on the (name of organization) Web site* OR *misplacement of five boxes, 250 paper medical records, during transit to a vendor destruction site].* The unsecured information includes *[list the types of information involved: part/complete medical records dated between (state date range), full name, Social Security Number, date of birth, home address, account number, diagnosis, types of treatment information, disability code, name other information types].*[4]

We recommend immediate steps be taken to protect *[yourself/your loved one]* from *[additional/potential]* information breach harm *[List fitting recommendations such as:*

- *Register a fraud alert with the three credit bureaus listed here; and order credit reports:*
  - *Experian: (888) 397-3742; www.experian.com; PO Box 9532, Allen, TX 75013*
  - *TransUnion: (800) 680-7289; www.transunion.com; Fraud Victim Assistance Division, PO Box 6790, Fullerton, CA 92834-6790*
  - *Equifax: (800)525-6285; www.equifax.com; PO 740241, Atlanta, GA 30374-0241*
- *Monitor account statements, EOBs, and credit bureau reports closely*
- *Contact the Consumer Protection Agency [Sample Google search for appropriate state: "consumer protection agency Illinois"]*
- *(If the consumer has validation their information has been compromised) Notify law enforcement to assist the investigation: [Provide advice on how to file and provide contact information for local law enforcement, the state attorney general office, and the Federal Trade Commission]*

- *Access helpful Web links to learn additional information on consumer protection when personal information is compromised. [List Web links or provide own organization's Web site] [For example, include AHIMA's Medical Identity Theft Response Checklist for Consumers: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_039114.pdf]*

[Name of responsible healthcare organization/s][5] [has/have taken OR *will soon take]* these steps to protect your, and others', personal information from further harm or similar circumstances: *[Choose from or customize these examples or add your own]:*

- *Initiated a forensics security investigation*
- *Filed a police report on [date]; Initiated a criminal investigation*
- *Sanctioned five employees/a physician by suspension/termination of employment/medical staff privileges*
- *Address operational or technology updates or changes triggered by the incident to improve confidentiality, such as strengthening technology safeguards or administrative policies and/procedures*
- *List steps a business associate is taking or investigation/cancellation of a business associate contract*
- *List any specific, relevant state law factors/directives*
- *Other*

State Law Customization Considerations—At appropriate points in the letter above, insert additional information required by state law such as:

- *Number of involved victims*
- *Potential level of threat to victims*
- *Possible future information security threats victims should be aware of*
- *The definition of PHI in your state*
- *What agencies were notified, such as state health department, state attorney general, and state police*

Furthermore, [name or responsible healthcare organization] is offering (you/name of individual) # years of free credit monitoring service. To take advantage of this offer, (give instructions to initiate the protection)].

[Name of responsible healthcare organization] sincerely apologizes for the inconvenience and concern this incident causes you. Your information privacy is very important to us and we will continue to do everything we can to correct this situation and fortify our operational protections for you and others.

You may contact us with questions and concerns in the following ways: *[by calling our Privacy Office at our toll free number (XXX) XXX-XXXX between the hours of X a.m. and X p.m., 24 hours or Monday to Friday; sending an e-mail message to xxxx@xxxx.org; addressing a letter to our postal address, Anywhere Hospital, 1234 Hospital Way, City, State].*

Sincerely,

[Name and title of an individual with knowledge of the incident]
[Contact information – may be the same as the contact information listed above]

C. Addendum C: Business Associate Security Incident Notification Letter Template

Re: Notice of Security Incident

Dear _____,

This letter is to provide you with notice of a security incident pursuant to the Business Associate Agreement dated [insert].

Our investigation is ongoing, and we will further supplement the information contained in this notice as we learn more.

What We Now Know

[Brief description of what occurred.]

ePHI and PII Compromised During the Attack

Based on the current information from the forensic investigation, and in accordance with our obligations under applicable law and our commitments defined in our Business Associate Agreements, we are notifying you that the current evidence indicates protected patient information was likely compromised during the attack. Based on current evidence, we believe the affected servers housed electronic Protected Health Information ("ePHI"), as defined by the Health Insurance Portability and Accountability Act ("HIPAA") and "personally identifiable information" and/or "personal information" ("PII") covered by applicable statutes, including but not limited to:

[List data elements impacted.]

Law Enforcement Involvement

[If law enforcement was contacted, state so here.]

Responsive Security Measures

In addition to our ongoing investigation into the security incident, we have [describe security measures taken to respond to the incident].

We sincerely regret that this incident occurred. We remain committed to serving you at the highest level and to working to assist you and all our customers in recovering from this attack.

Sincerely,

_____

D. **Addendum D: Person and Identity Verification Table**

Person to Identify	**In-Person Encounter**	**Telephone Encounter**	**Request in Writing** (Fax, mail, hand-delivered)
Attorney	▪ Presents business card and photo identification (*i.e.,* driver's license or organization ID badge).	▪ It would be difficult to verify identity and authority by phone. Verification in person or in writing may be required.	▪ Supplies business card, photo identification (*i.e.,* driver's license or org ID badge), and letterhead. Confirmation call is required.
Facility Directory	▪ Verify identity	▪ Verify identity	▪ Verify identity
Patient	▪ Patient provides name, address, and date of birth and/or social security number; or ▪ Acquainted with patient.	▪ Patient provides name, address, and date of birth and/or social security number; or ▪ Acquainted with patient.	▪ Patient provides name, address, and date of birth and/or social security number. Verify patient's signature with that on file or on driver's license.
Personal Representative (Legal Guardian) for the Patient	▪ Personal Rep provides patient's name, address, and date of birth and/or social security number, **and** verifies (via legal docs) relationship to patient; or, ▪ Acquainted with personal Rep as such.	▪ Personal Rep provides patient's name, address, and date of birth and/or social security number, **and** verifies (via legal docs) relationship to patient; or, ▪ Acquainted with Personal Rep as such.	▪ Personal Rep provides patient's name, address, and date of birth and/or social security number. Verify the Personal Rep's signature with signature on file or on driver's license.
Persons Involved in the Patient's Immediate Care (PHI relevant only to the patient's current care) ▪ Blood Relative ▪ Spouse ▪ Domestic Partner ▪ Roommate ▪ Significant Other ▪ Neighbor ▪ Colleague	▪ Patient actively involves this person in his/her care; or ▪ In your best professional judgment, the disclosure is in the patient's best interest.	▪ Patient actively involves this person in his/her care; or ▪ In your best professional judgment, the disclosure is in the patient's best interest. ▪ Use call-back.	▪ N/A
Power of Attorney ("POA") For the Patient	▪ Presents a photo ID and a copy of the POA. Verify patient's signature with one on file. ▪ Acquainted with POA as being such.	▪ Previously obtained a copy of the POA and verified the patient's signature with one on file. ▪ Acquainted with POA as being such.	▪ Obtain a copy of the POA and verify the patient's signature with the one on file.
Provider From Another Facility	▪ Acquainted with provider as a treatment provider; ▪ Provider is wearing a photo badge from his/her facility; or, ▪ Patient/personal representative	▪ Acquainted with provider as a treatment provider; or; ▪ Call requestor back through their facility's main switchboard number (not via a direct number).	▪ Recognize name of facility and address on letterhead as a treatment facility; or ▪ Call requestor back through their facility's main switchboard number (not via a direct number).

Person to Identify	In-Person Encounter	Telephone Encounter	Request in Writing (Fax, mail, hand-delivered)
	introduces provider to you.		
Public Official ▪ CIA ▪ Court Order ▪ FBI ▪ Law Enforcement Officer ▪ OCR ▪ OIG ▪ Public Health Agency Official ▪ Other	▪ Presents an agency I.D. badge; ▪ Presents with a written statement of legal authority; ▪ Presents with a written statement of appointment on appropriate govt. letterhead; ▪ Presents warrant, court order, or legal process issued by a grand jury, or a judicial or admin. tribunal; ▪ Presents with a contract for services or purchase order; or, ▪ Official states release is necessary to prevent or lessen the threat to the health/safety of a person/public.	▪ Official states release is necessary to prevent or lessen the threat to the health/safety of a person/public.	▪ Written statement of legal authority; ▪ Written statement of appointment on appropriate government; ▪ Warrant, court order, or other legal process issued by a grand jury or a judicial or administrative tribunal; or ▪ Contract for services or purchase order.
Vendor Who Helps Assists w Treatment, Payment, or Health Care Operations Examples include, but are not limited to the following: ▪ Accreditation Org. ▪ DME Company ▪ Insurance Co. ▪ Pharmacy Vendor Bioventus has a Rebate Agreement with ▪ Software Vendor ▪ Statement Vendor	▪ Recognize requestor/ organization; or ▪ Photo identification with organization.	▪ Recognize requestor or organization.	▪ Recognize requestor/ organization; or ▪ Call requestor back through their facility's main switchboard number (not via a direct number).
Workforce Member of Our Organization	▪ Acquainted with individual as a workforce member; or, ▪ Workforce member is wearing an I.D. badge.	▪ Acquainted with individual as a workforce member; or, ▪ Workforce member is calling from an in-house extension.	▪ Request is sent from/through our own computer system; or ▪ Request is on our own letterhead.

E. **Addendum E: PHI Disclosure Table**

Requestor	Authorization Required?	Copy Fee Charged?	Track on Disclosure Accounting?
Accrediting Agencies (JCAHO, CARF)	No	No	No
Attorney for Resident	Yes	Yes	No
Attorney for Facility/Corporation	No	No	No
Contractors/ Business Associates	No, unless their purpose falls outside of TPO.	No	No
For Deceased Persons ▪ Coroner or Medical Examiner, Funeral Directors ▪ Organ Procurement	No	No	Yes
Employer ▪ PHI specific to work related illness or injury, and ▪ Required for employer's compliance with occupational safety and health laws.	No, for the purpose listed. Yes, for all others.	No	No
Family Members	No for oral disclosures to family members involved in care; Yes, for others.	Yes	No
Entity Subject to the Food and Drug Administration ("FDA") ▪ Adverse events, product defects or biological product deviations ▪ Track products ▪ Enable product recalls, repairs, or replacements ▪ Conduct post marketing surveillance	No	No	Yes
Health Oversight ▪ Government benefits program ▪ Fraud and abuse compliance ▪ Civil rights laws ▪ Trauma/tumor registries ▪ Vital statistics ▪ Reporting of abuse or neglect	No	No	Yes
Health Care Practitioners and Providers for Continuity of Treatment and Payment	No	No	No
Health Care Practitioners and Providers if <u>not</u> Involved in Care or Treatment (*i.e.*, consultants)	No	No	No
Insurance Companies/Third-Party Payors ▪ Related to Claims Processing	No	No	No

Requestor	Authorization Required?	Copy Fee Charged?	Track on Disclosure Accounting?
Judicial and Administrative Proceedings ▪ Court order, or warrant ▪ Subpoena	No No	No Yes	Yes Yes
Law Enforcement ▪ Administrative request ▪ Locating a suspect, fugitive, material witness, or missing person ▪ Victims of crime ▪ Crimes on premises ▪ Suspicious deaths ▪ Avert a serious threat to health or safety	No	No	Yes, except for disclosures to correctional institutions.
Public Health Authorities ▪ Surveillance ▪ Investigations ▪ Interventions ▪ Foreign governments collaborating with US public health authorities ▪ Recording births/deaths ▪ Child/elder abuse ▪ Prevent serious harm ▪ Communicable disease	No	No	Yes
Research (w/o Authorization)	No, if IRB or Privacy Board approves research study and waives authorization.	No	Yes
Resident/Resident's Personal Representative	No	Yes	No
Specialized Government Functions ▪ Military and Veterans' activities ▪ Protective services for the President ▪ Foreign military personnel ▪ National security and intelligence activities	No	No	Yes, except for disclosures for national security and intelligence activities.
Workers' Compensation ▪ Comply w/existing laws (see state law)	No	See applicable state law.	Yes

F. Addendum F: Sample Data Use Agreement - Annotated

DATA USE AGREEMENT

This Data Use Agreement ("Agreement"), effective as of this _____ day of _____, 20__ ("Effective Date"), is entered into by and between _____ ("Recipient") and _____ ("Covered Entity"). The purpose of this Agreement is to provide Recipient with access to a Limited Data Set ("LDS") for use in its Research and Public Health analyses and for the Health Care Operations of the Covered Entity, in accordance with HIPAA Regulations.

> **Comment**: Assuming that the patient has not executed an Authorization and other HIPAA exceptions do not apply, a Covered Entity disclosing PHI and a vendor receiving PHI will need to execute either a Business Associate Agreement ("BAA"), or a Data Use Agreement ("DUA"), but not both.

1. **Definitions.** Unless otherwise specified in this Agreement, all capitalized terms used in this Agreement not otherwise defined have the meaning established for purposes of the "HIPAA Regulations" codified at Title 45 parts 160 through 164 of the United States Code of Federal Regulations, as amended from time to time.

2. **Preparation of the LDS**. Covered Entity shall prepare and furnish to Recipient an LDS in accord with the HIPAA Regulations or Covered Entity shall retain Recipient as a Business Associate (pursuant to an appropriate Business Associate Agreement) and direct recipient, as its Business Associate, to prepare such LDS.

3. **Minimum Necessary Data Fields in the LDS**. In preparing the LDS, Covered Entity or its Business Associate shall include the data fields specified by the parties from time to time, which are the minimum necessary to accomplish the purposes set forth in Section 5 of this Agreement.

4. **Responsibilities of Recipient**. Recipient agrees to:

a. Use or disclose the LDS only as permitted by this Agreement or as required by law;

> **Comment**: The parties can also articulate that Recipient's use of the LDS will be limited to the minimum necessary to accomplish the purposes of the disclosure from the Covered Entity to the Recipient.

b. Use appropriate safeguards to prevent use or disclosure of the LDS other than as permitted by this Agreement or required by law;

> **Comment**: A Covered Entity may want to require that the Recipient document such safeguards and agree to keep them current and updated.

c. Report to Covered Entity any use or disclosure of the LDS of which it becomes aware that is not permitted by this Agreement or required by law;

> **Comment**: The DUA can add further specificity to this reporting requirement by, for instance, requiring notification to the Covered Entity upon disclosure to an unauthorized subcontractor (*see* comment to Section 5, below) or adding a timing requirement for the notification. This provision also can provide specific instructions on notification, such as where to send the notification and who is the point of contact. It can also specify the information that the Covered Entity desires, including the nature of the issue, the unauthorized user or recipient and the corrective action or mitigation steps taken by the recipient.

d. Require any of its subcontractors or agents that receive or have access to the LDS to agree to the same restrictions and conditions on the use and/or disclosure of the LDS that apply to Recipient under this Agreement; and

e. Not use the information in the LDS to identify or contact the individuals who are data subjects.

5. **Permitted Uses and Disclosures of the LDS**. Recipient may use and/or disclose the LDS for its Research and Public Health activities and the Health Care Operations of the Covered Entity.

> **Comment**: The parties can add further specificity to this section, as necessary. For example, the parties can add specific details regarding the particular research project or the particular purpose for which the recipient party seeks the data. The DUA also can place limitations on others (such as subcontractors) who are permitted to use or receive the LDS.

6. **Term and Termination**.

a. Term. The term of this Agreement shall commence as of the Effective Date and shall continue for so long as Recipient retains the LDS, unless sooner terminated as set forth in this Agreement.

b. Termination by Recipient. Recipient may terminate this Agreement at any time by notifying the Covered Entity and returning or destroying the LDS.

c. Termination by Covered Entity. Covered Entity may terminate this Agreement at any time by providing thirty (30) days prior written notice to Recipient.

d. For Breach. Covered Entity shall provide written notice to Recipient within ten (10) days of any determination that Recipient has breached a material term of this Agreement. Covered Entity shall afford Recipient an opportunity to cure said alleged material breach upon mutually agreeable terms. Failure to agree on mutually agreeable terms for cure within thirty (30) days shall be grounds for the immediate termination of this Agreement by Covered Entity.

> **Comment**: A Covered Entity may want to require a recipient to mitigate any harmful effect of a use or disclosure of the LDS that is in violation of the DUA. The Covered Entity also should consider requiring the recipient to bear the burden of any costs related to mitigating or remedying a violation of the Agreement. The parties also can add a termination provision specifying that the Agreement will terminate immediately, if necessary, to comply with a change in law or regulation.

e. Effect of Termination. Sections 1, 4, 5, 6(e), and 7 of this Agreement shall survive any termination of this Agreement under Sections 6(c) or 6(d).

> **Comment**: The parties should consider addressing return or destruction of the LDS provided to the recipient, such as by requiring that the Recipient return the data to the Covered Entity or destroy the data, with certification from Recipient to the Covered Entity. As in many BAAs, the parties can include a provision that, if return or destruction is infeasible, the Recipient will extend the protections required by the DUA to the LDS and only use the LDS for the purposes that make the return or destruction of the information infeasible.

7. **Miscellaneous**.

a. Change in Law. The parties agree to negotiate in good faith to amend this Agreement to comport with changes in federal law that materially alter either or both parties' obligations under this Agreement. Provided however, that if the parties are unable to agree to mutually acceptable

amendment(s) by the compliance date of the change in applicable law or regulations, either Party may terminate this Agreement as provided in Section 6.

> **Comment**: As stated in the comment to Section 6(d), the parties can consider modifying or strengthening this provision to allow for immediate termination for a change in law or regulation.

b. Construction of Terms. The terms of this Agreement shall be construed to give effect to applicable federal interpretative guidance regarding the HIPAA Regulations.

c. No Third-Party Beneficiaries. Nothing in this Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

d. Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

e. Headings. The headings and other captions in this Agreement are for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this Agreement.

_____
(Covered Entity)

By: _____
(Signature)

Name: _____
(Print)

Title: _____

_____
(Recipient)

By: _____
(Signature)

Name: _____
(Print)

Title: _____

G. **Addendum G: HIPAA Risk Assessment Analysis and Methodology per OCR Guidance**

1. Risk Analysis Requirements under the Security Rule

- **The Security Management Process** standard in the Security Rule requires Bioventus to "implement policies and procedures to prevent, detect, contain, and correct security violations." Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard. Section 164.308(a)(1)(ii)(A) states:
    - **Risk Analysis** (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information ("e-PHI") held by [the organization].
- The outcome of the risk analysis process is a critical factor in assessing whether an implementation specification or an equivalent measure is reasonable and appropriate.
- Bioventus should use the information gleaned from its risk analysis when it, for example:
    - Designs appropriate personnel screening processes;
    - Identifies what data to backup and how;
    - Decides whether and how to use encryption;
    - Addresses what data must be authenticated situations to protect data integrity; or
    - Determines the appropriate manner of protecting health information transmissions.

Important Definitions

- Unlike "availability," "confidentiality," and "integrity," the following terms are not expressly defined in the Security Rule. The definitions provided in this Addendum (based on HHS guidance), which are consistent with common industry definitions, are provided to put the risk analysis discussion in context.
- **Vulnerability**. Vulnerability is defined in NIST Special Publication (SP) 800-30 as "a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy." Vulnerabilities, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as inappropriate access to or disclosure of PHI. Vulnerabilities may be grouped into two general categories, technical and nontechnical. Non-technical vulnerabilities may include ineffective or non-existent policies, procedures, standards, or guidelines. Technical vulnerabilities may include holes, flaws, or weaknesses in the development of information systems, or incorrectly implemented and/or configured information systems.
- **Threat**. An adapted definition of threat from NIST SP 800-30 is "the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability." There are several types of threats that may occur within an information system or operating environment. Threats may be grouped into general categories such as natural, human, and environmental. Examples of common threats in each of these general categories include:
    - Natural threats such as floods, earthquakes, tornadoes, and landslides;
    - Human threats, enabled or caused by humans, such as actions that are intentional (*e.g.,* network and computer-based attacks, malicious software upload, and unauthorized access to ePHI) or unintentional (*e.g.,* inadvertent data entry or deletion, or inaccurate data entry); and
    - Environmental threats such as power failures, pollution, chemicals, and liquid leakage.

- **Risk**. An adapted definition of risk from NIST SP 800-30 is, "The net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur… Risks arise from legal liability or mission loss due to (1) unauthorized (malicious or accidental) disclosure, modification, or destruction of information, (2) unintentional errors and omissions, (3) IT disruptions due to natural or man-made disasters, and (4) failure to exercise due care and diligence in the implementation and operation of the IT system."
    - Risk can be understood as a function of (1) the likelihood of a given threat triggering ore exploiting a vulnerability and (2) the resulting impact on Bioventus. This means that risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.

2. Elements of a Risk Analysis

There are numerous methods of performing risk analysis and there is no single method that guarantees compliance with the Security Rule. Some examples of steps that might be applied in a risk analysis process are outlined in NIST SP 800-30.6.

3. Scope of the Risk Analysis

The scope of risk analysis that the Security Rule encompasses includes the potential risks and vulnerabilities to the confidentiality, availability, and integrity of all e-PHI that Bioventus creates, receives, maintains, or transmits. This includes e-PHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, smart phones, transmission media, or portable electronic media. Thus, risk analysis should consider all Bioventus' e-PHI, regardless of the particular electronic medium in which it is created, received, maintained, or transmitted, or the source or location of its e-PHI.

- **Data Collection**. Bioventus must identify and document where the e-PHI is stored, received, maintained, or transmitted.
- **Identify and Document Potential Threats and Vulnerabilities**. Bioventus must identify and document reasonably anticipated threats to e-PHI. Bioventus may identify different threats that are unique to the circumstances of their environment. Bioventus must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI.
- **Assess Current Security Measures**. Bioventus should assess and document the security measures an entity uses to safeguard e-PHI, whether security measures required by the Security Rule are already in place, and if current security measures are configured and used properly.
- **Determine the Likelihood of Threat Occurrence**. The Security Rule requires Bioventus to consider the probability of potential risks to e-PHI. The results of this assessment, combined with the initial list of threats, will influence the determination of which threats HIPAA requires protection against because they are "reasonably anticipated." The output of this part should be documentation of all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability, and integrity of e-PHI of Bioventus.
- **Determine the Potential Impact of Threat Occurrence**. HIPAA also requires consideration of the "criticality," or impact, of potential risks to confidentiality, integrity, and availability of e-PHI. Bioventus must assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability. An entity may use either a qualitative or

quantitative method or a combination of the two methods to measure the impact on the organization. The output of this process should be documentation of all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability, and integrity of e-PHI within Bioventus.

- **Determine the Level of Risk**. Bioventus should assign risk levels for all threat and vulnerability combinations identified during the risk analysis. The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination might be performed by assigning a risk level based on the average of the assigned likelihood and impact levels. The output should be documentation of the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level.
- **The Math**. A common way to perform this assessment is the risk equation:
  - **Risk = Threat x Vulnerability x Asset**
- **Finalize Documentation**. The Security Rule requires the risk analysis to be documented but does not require a specific format. The risk analysis documentation is a direct input to the risk management process. Tables such as the one below can be a useful way to visualize and document assessments.

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Control Recommendations
System failure — Overheating in server room High	Air-conditioning systems is ten years old. High	Servers Critical	All services (website, email, etc.) will be unavailable for at least 3 hours. Critical	High Current temperature in server room is 40C	High Potential loss of $50,000 per occurrence	Buy a new air conditioner, $3,000 cost.
Malicious human (interference) — DDOS attack. High	Firewall is configured properly and has good DDOS mitigation. Low	Website Critical	Website resources will be unavailable. Critical	Medium DDOS was discovered once in 2 years.	Medium Potential loss of $10,000 per hour of downtime	Monitor the firewall.
Natural disasters — Flooding High	Server room is on the 3rd floor. Low	Servers. Critical	All services will be unavailable. Critical	Low Last flood in the area happened 10 years ago.	Low	No action needed.
Accidental human interference — Accidental file deletions High	Permissions are configured properly; IT auditing software is in place; backups are taken regularly. Low	Files on a file share Medium	Critical data could be lost but almost certainly could be restored from backup. Low	Medium	Low	Continue monitoring permissions changes, privileged users and backups.

- **Periodic Review and Updates to the Risk Assessment**. The risk analysis process should be ongoing. For an entity to update and document its security measures “as needed,” which HIPAA requires, it should conduct continuous risk analysis to identify when updates are needed.

H. **Addendum H: HIPAA Authorization Form - Sample**

HIPAA AUTHORIZATION FOR USE OR DISCLOSURE OF HEALTH INFORMATION

This form is for use when such authorization is required and complies with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Standards.

Print Name of Patient: _____

Date of Birth: _____ SSN: _____

I. My Authorization

I authorize the following using or disclosing party:

_____

to use or disclose the following health information.

☐ - All of my health information

☐ - My health information relating to the following treatment or condition:

_____

☐ - My health information covering the period from _____ (date) to _____ (date)

☐ - Other: _____

The above party may disclose this health information to the following recipient:

Name (or title) and organization _____

Address _____

City _____ State _____ Zip _____

Phone _____ Fax _____ Email _____

The purpose of this authorization is (check all that apply):

☐ - At my request

☐ - Other: _____

☐ - To authorize the using or disclosing party to communicate with me for marketing purposes when they receive payment from a third party to do so.

☐ - To authorize the using or disclosing party to sell my health information. I understand that the seller will receive compensation for my health information and will stop any future sales if I revoke this authorization.

This authorization ends:

☐ - On (date)_____

☐ - When the following event occurs: _____

Page 1 of 3

II. My Rights

I understand that I have the right to revoke this authorization, in writing, at any time, except where uses or disclosures have already been made based upon my original permission. I may not be able to revoke this authorization if its purpose was to obtain insurance. In order to revoke this authorization, I must do so in writing and send it to the appropriate disclosing party.

I understand that uses and disclosures already made based upon my original permission cannot be taken back.

I understand that it is possible that information used or disclosed with my permission may be re-disclosed by the recipient and is no longer protected by the HIPAA Privacy Standards.

I understand that treatment by any party may not be conditioned upon my signing of this authorization (unless treatment is sought only to create health information for a third party or to take part in a research study) and that I may have the right to refuse to sign this authorization.

I will receive a copy of this authorization after I have signed it. A copy of this authorization is as valid as the original.

Signature of Patient: _____

Date: _____

If the patient is a minor or unable to sign, please complete the following:

☐ - Patient is a minor: _____ years of age

☐ - Patient is unable to sign because: _____

Signature of Authorized Representative: _____

Date: _____

Print Name of Authorized Representative: _____

Authority of representative to sign on behalf of the patient:

☐ - Parent ☐ - Legal Guardian ☐ - Court Order ☐ - Other: _____

III. Additional Consent for Certain Conditions

This medical record may contain information about **physical or sexual abuse, alcoholism, drug abuse, sexually transmitted diseases, abortion, or mental health treatment**. Separate consent must be given before this information can be released.

☐ - I consent to have the above information released.

☐ - I do not consent to have the above information released.

Signature of Patient or Authorized Representative: _____

Date: _____ Time: _____

IV. Additional Consent for HIV/AIDS

This medical record may contain information concerning **HIV testing and/or AIDS diagnosis or treatment**. Separate consent must be given to have this information released.

☐ - I consent to have the above information released.

☐ - I do not consent to have the above information released.

Signature of Patient or Authorized Representative: _____

Date: _____ Time: _____