HIPAA Manual

Owner Name: Process Excellence Team (PeX)

Version: 2.0

neurealm

Document History

Version	Date	Summary of Changes	Author	Approved By
1.0	13th Feb 2017	Initial Version	Sekar T	CDO
1.01	27th Apr 2017	Change in Security Personnel – Sekar T will play the role in the place of Hariharan Madhavan	Sekar T	CDO
1.02	15-Jan-18	Annual Policy review – No changes to IS policies	Sekar T	Security Council
1.03	19-Mar-19	1. Annual Policy review – No changes to policies 2. Continual Improvement :– Implementation of Advanced Threat Protection	Sekar T	Quality Council
1.04	02-April-19	1. Scope Extension - Inclusion of Premier Inc., account under the section Scope	Sekar T	CCSO
1.05	23-April-19	1. Change in the name of Security Official – From Sekar to Hariram 2. Continual Improvement :– Implementation of a. Endpoint Protection with User Behaviour Analysis(UBA) and DLP Rules to alert SOC team on suspicious behaviour b. Mobile device management to securely access email c. Office 365 DLP rules to monitor file attachments for sensitive information.	Sekar T	CCSO
1.06	02-May-19	1. Included appropriate wordings for the annual refresher training that is currently practiced 2. Ensure all the new hires are trained and completed assessment on HIPAA and Information Security Management System (ISMS) within 30 days from the date of joining	Sekar T	Security Council

		Neurealm or from the date the course is assigned to the employee for the annual refresher training 3. The statement underlined above is included 4. CI – Implementation of a. Virtual Desktop Interface(VDI) to securely access client environment in healthcare projects. b. Mobile Device Management		
1.07	09-Dec-19	1. Change in the name of Security Official – From Hariram to Hariharan Madhavan 2. CI – Implementation of a. Cloud Storage sites are blocked unless specifically used by the client environments for business apps b. Our endpoint security includes a NGAV(Next Generation Antivirus and Endpoint Detection and Response	Sekar T	Security Council
1.08	09-Mar-20	Annual Policy review – No changes to policies	Shivaram J	Security Council
1.09	30-July-20	CI – Implementation of Azure Sentinel	Sekar T	Security Council
1.10	26-May-21	Change of Head of SOC – Hariharan G to Kannan Srinivasan	Sekar T	Balaji Uppili
1.11	18-Apr-22	Annual Policy review – No changes to manual	Sekar T	Balaji Uppili
1.12	30-Apr-23	Annual Policy review – No changes to manual	Sekar T	Balaji Uppili
1.13	20-12-2024	Annual Policy Review - Updated accounts that are applicable for HIPAA under the Covered functions	Shalot Leely	COO

2.0	13-05-2025	Company name and logo change	Shalot Leely M	Ambrish S

Contents

I.Introduction

This document describes the HIPAA Policy, associated policies and procedures implemented at Neurealm. This document is part of Neurealm Business Management System that is documented in Neurealm BMS Manual.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its regulations limit Neurealm ("Company") abilities to use and disclose protected health information (PHI). The statements in this manual represent Neurealm' policies and procedures related to HIPAA.

Protected health information means information that is created or received by the Company and relates to the past, present, or future physical or mental health condition of a Patient/Client ("Participant"); the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. Protected health information includes information of persons living or deceased.

Some examples of PHI are:

- *Participant's medical record number*
- *Participant's demographic information (e.g. address, telephone number, fax #, email id)*
- *Information doctors, nurses and other health care providers put in a participant's medical record*
- *Images of the participant*
- *Appointment dates / times*
- *Lab results*
- *Visit documentation*
- *Conversations a provider has about a participant's care or treatment with nurses and others*
- *Information about a participant in a provider's computer system or a health insurer's computer system*
- *Billing information about a participant at a clinic*
- *Any health information that can lead to the identity of an individual or the contents of the information can be used to make a reasonable assumption as to the identity of the individual*

II. Definitions

A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity. The Privacy Rule lists some of the functions or activities, as well as the services, that make a person or entity a business associate, if the activity or service

involves the use or disclosure of protected health information. The types of functions or activities that may make a person or

entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.

Note: Business Associate Decision Tree that is available in reference section of this document shall be used to determine the need for Business Associate agreement

See the definition of “business associate” at 45 CFR 160.103.

Covered Entity means a health plan, a health care clearing house, or a health care provider who transmits health information in electronic form in connection with a transaction for which the U.S. Department of Health and Human Services has adopted a standard. 45 C.F.R. 160.103

Health Care Clearinghouse means a public or private entity, including a billing service, re- pricing company, community health management information system or community health information system, and “value-added” networks and switches, that does either of the following functions

HHS stand for the Department of Health and Human Services CFR stand for Code of Federal Regulations

PR stand for Privacy Rule

Breach is impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.

III.General Policy

Neurealm is committed to protect the privacy of Individual health information in compliance with the HIPAA and the regulations disseminated there under. These policies and procedures along with ISMS policies, Code of Conduct and procedures shall be applied to safeguard the protected health information created, stored, acquired, transmitted or maintained by the designated functions of Neurealm.

All workforce who have access to PHI (includes ePHI) must comply with this General Policy and other policies and procedures laid out in this document. The workforce include individuals who would be considered as part of the workforce under HIPAA such as staff, employees, volunteers, interns and other persons whose work performance is under the direct control of Neurealm, whether they are paid by the Neurealm. All members of Neurealm expected to report potential fraud, waste and abuse to complianceofficer@Neurealm.com

Security & Privacy Risk Assessment shall be carried out as per the standard practice applicable for Risk Management

HIPAA Compliance Objectives

The following are the objectives applicable for all Health Care projects that deal with PHI.

All Health Care Projects - PM	Ensure all the new hires are trained and completed assessment on HIPAA and Information Security Management System (ISMS) within 30 days from the date of joining Neurealm or from the date the course is assigned to the employee for the annual refresher training
	Risks Assessment is carried out at least once in a Quarter
	Ensure 100% compliance to HIPAA Policies & Practices
SOC & IT	SOC - Internal Vulnerability Assessment is carried out once in a Quarter for all Health Care projects IT - Security patches that are published by OEM and security gaps reported by Neurealm SOC are remediated as per SLA
Compliance - Internal Audit Function	Ensure all health care projects are audited at least once in a Half Year(Financial Calendar)
Customer Success Manager	All incidents and breaches related to HIPAA are handled within the timeline

Note: The above stated objectives along with security objectives stated in the ISMS Policy would be measured and reviewed as part of Security Council meeting.

IV. Scope

These policies and procedures apply only for the designated function that is managing Health Care projects, which include:

Delivery / Service Support – Covered functions

- Delivery – Infrastructure Management Service (IMS)
- Delivery – Application Development & Maintenance

Business Support – Non-Covered functions

- Admin Support
- IT Support
- SOC
- Quality
- Solutions & Strategy
- Internal Audit
- HR Support
- Training – (Neurealm Learning Academy)

List of accounts / projects that are applicable for HIPAA under the Covered functions

S. No.	Account / Customer
1	The Jewish Board
2	BLHC
3	Tufts Medicine
4	Covenant Health
5	ZOLL
6	Embecta MEDICAL II LLC
7	Premier Inc. – Application Development, Maintenance and Support & Infrastructure Management Services
8	ZIF
9	ESSEN CARE MANAGEMENT
10	CINQ CONNECT
11	BCBSA

The designated covered functions may not share protected health information with the non-covered functions of the company (Neurealm) and any other third parties even if NDA exist, unless specifically permitted by the privacy regulations or business associates agreement. It is the responsibility of each designated covered function to assure that their employees, staff, contractors etc., comply with these policies and procedures. Similarly work force of business support Non-covered functions shall not access ePHI

V. General Policies and Procedures

1. Authorization to use or disclose protected health information

a. Policy

Covered entity will obtain an individual's authorization to use or disclose PHI in accordance with HIPAA. Business Associate (Neurealm) will not use or disclose protected health information unless it is authorized by covered entity.

b. Procedure

- Business Associate (Neurealm) shall have a written authorization with the following details a) Authorized Signatory Name b) Purpose of authorization to use or disclose of ePHI.
- Business Associates (Neurealm) must retain any signed / digital authorization

c. Documentation

The Business Associate must document and retain any signed authorization and maintain such records in the project repository

d. Applicable Regulations

45.C.F.R 164.508, 164.512

2. Business Associates

a. Policy

Business Associates may share protected health information with external parties as agreed in the business associates agreement or any other form of agreement signed with covered entity.

Note: Business Associate Decision Tree that is available in reference section of this document shall be used to determine the need for Business Associate agreement.

b. Procedure

a) Business Associate Agreement template is made available with Neurealm Finance / Legal team, the same must be used to sign between Neurealm and covered entity or a business associate. In case covered entity supply the BA agreement template, the clauses / terms that are not covered shall be resolved by the concerned person and approved by Neurealm Privacy Officer

a) Generally, PHI may only be shared with business associates pursuant to a valid Business Associate Agreement

b) Business Associate Agreement must be in writing and must contain English language that is HIPAA complian

c. Applicable Regulations
45 C.F.R. 164.502(e), 164.504(e), 164.532,160

3. Complaint

a. Policy

An individual who believes his or her HIPAA privacy rights have been violated may file a complaint regarding the suspected privacy violation with the Privacy Officer of covered entity first, where it is not resolved Official of the appropriate Office of Civil Rights (OCR) Regional office. Complaints submitted by covered entity to the Neurealm Privacy Official will be documented, reviewed and acted upon, if necessary.

b. Procedure

Filing a complaint

1. Covered entities and business associates shall submit a complaint using the compliant form applicable for the covered entity or business associate.
2. The complaint must name the entity that is the subject of the compliant and describe the acts or omission believed to be in violation of the HIPAA requirements

Investigation, Response and Sanctions

3. The Neurealm Privacy Official shall investigate suspected or reported complaints following through the Incident Management process to determine if a breach of privacy has occurred or any potential instance of breach, fraud, waste & abuse. Neurealm Privacy Official shall complete HIPAA Breach/Risk Assessment worksheet as part of the investigation.
4. Neurealm Privacy Official shall submit an Incident report with root cause analysis to the Privacy Officer of Covered Entity / Business Associate within five business days
5. If the Neurealm Privacy Official determines that a violation occurred, the Privacy Official will notify concerned department and HR to follow through the Incident Management procedure that include initiating disciplinary process against the person or entity who failed to comply with the privacy policies and procedures and instruct the person or entity to take the corrective action

c. Applicable Regulations

45 C.F.R 160.304, 160.306, 160.308, 160.310, 160.410, 164

4. De-Identification of Protected Health Information

a. Policy

The Neurealm may use de-identified PHI for covered entity without obtaining an individual's authorization. PHI shall be considered de-identified if either of the two de-identification procedure set forth below are followed.

b. Procedure

Removal of Identifiers

- De-identified PHI is rendered anonymous when identifying characteristics are completely removed and when the company does not have any actual knowledge that the information could be used alone or in combination with other information to identify and individual
- De-identification requires the elimination not only of primary or obvious identifiers, such as individual's name, address, and date of birth, but also of secondary identifiers through which a user could deduce the individual's identity.
- For information to be de-identified the following identifiers must be removed;
  - Names
  - All address information except for the state;
  - Names of the relatives and employers;
  - All elements of dates, including date of birth, admission date, discharge date, date of death;
  - Telephone numbers;
  - Fax numbers;
  - E-mail addresses;
  - Social Security numbers;
  - Medical record numbers;
  - Health Plan beneficiary numbers;
  - Account numbers;
  - Certificate/License numbers
  - Vehicle identifiers
  - Biometric identifiers
  - Full face photographic images and other comparable images;
  - Any other unique identifying number characteristics

c. Re-identification

A covered component may assign a code or other means of record identification to allow information de-identified under this section to be re- identified by the covered component, provided the code or other means of record identification is not derived from the information about the individual. The covered component shall not disclose the mechanism for re-identification to others

d. Applicable Regulations

45 C.F.R 164.502(d), 164.514(a) and (b)

5. Limited Data Sheet

a. Policy

The designated covered functions may use protected health information to create a limited data set, or to disclose protected health information to the covered entity. The designated covered functions may use and disclose a limited data set without an individual's authorization for health care operations.

b. Procedure

A limited data set is PHI that excludes the following direct identifiers of the individual or relatives, employers, or household members of the individual:

- Names;
- All address information other than town, city, state, and zip codes;
- Telephone numbers;
- Fax numbers;
- E-mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health Plan beneficiary numbers;
- Account numbers;
- Certificate/License numbers
- Vehicle identifiers
- IP address numbers;
- Biometric identifiers
- Full face photographic images and other comparable images

Data Use Agreements. Data use agreements must:

1. Establish the permitted uses and disclosures of the limited data set;
2. Establish who is permitted to use or receive the limited data set; and
3. Provide that the recipient of the information will;
   a) Not use or further disclose the information other than as permitted by the agreement;
   b) Use appropriate safeguards to prevent use or disclose other than as permitted by the agreement;
   c) Report to covered entity any uses or disclosure that recipient is aware of that that is provided by the agreement
   d) Ensure that the recipient's agents who have access to the information
   e) agree to the same restrictions as imposed on the recipient; and
   f) Not identify the information or contact the individuals

c. Applicable Regulations

45 C.F.R 164.514 (e)

5. Minimum Necessary Use and Disclosure of Protected Health Information

a. Policy

When using, or disclosing PHI or when requesting PHI from another entity covered by HIPAA privacy regulations, the company (Neurealm) shall make a reasonable effort to limit itself to the minimum amount of protected health information necessary to accomplish the intended purpose of the use, disclosure or request upon obtaining an approval from covered entity. Neurealm will not disclose PHI even under the following circumstances unless it is authorized by concerned approving authority of covered entity :

- ❖ For Treatment: - Disclosure to or request by a health care provider for diagnosing or treating an individual
- ❖ To the Individual: - Uses or disclosures made to the individual.
- ❖ Pursuant to Patient's Authorization: - Uses or disclosure pursuant to a valid authorization.
- ❖ To the HHS :- Disclosure to the Office for Civil Rights of the U.S Department of Health and Human Services for HIPAA compliance purposes
- ❖ Required by Law :- Uses or disclosures that are required by law

b. Procedures

The company (Neurealm) recognizes that each designated covered component that uses or discloses protected health information has a unique organizational structure and that employees of the unit may perform various functions for the unit that require different levels of access to protected health information. Further, the responsibilities designate to these functions vary across each designated covered component at the company. It is the responsibility of delivery manager to ensure that the access granted are appropriate.

For any type of disclosure that it makes on a routine and recurring basis, Business Associate (designated covered functions) shall obtain one time authorization from the covered entities

c. Applicable Regulations

45 C.F.R 164.502, and 164.514(d)

6. Notice of Privacy Practices

a. Policy

Neurealm is committed to maintaining and protecting the confidentiality of the individual's PHI. This Notice of Privacy Practices applies to Neurealm and required to comply with the Health Insurance Portability and Accountability Act ("HIPAA") to protect the individual's PHI and other personal information. Where required Neurealm shall provide the individual with this Notice of Privacy Practices about the Neurealm's policies, safeguards, and practices. When Neurealm uses or discloses an individual's PHI,

Neurealm is bound by the terms of this Notice of Privacy Practices, or the revised Notice of Privacy Practices, if applicable.

b. Procedure

Neurealm will use PHI as agreed with covered entity and will not disclose PHI to any other third parties. The individual may revoke such permission at any time by writing to Privacy Officer of covered entity.

c. Applicable Regulations

45 C.F.R 164.520

7. Privacy Official, Security Officer, and Privacy coordinators

a. Privacy Official

Neurealm has designated a Privacy Official who is responsible for the development and implementation of the Neurealm's policies and procedures related to the privacy and security of PHI under HIPAA.

Responsibilities of the Privacy Official include:

1. Maintain ongoing communication with Security Official (SOC) and all Privacy Coordinators (Project Manager or Team Lead or Team Member as appointed by Delivery manager)
2. Coordinate training programs for the designated covered functions in cooperation with Privacy Coordinators
3. Respond to complaints regarding Neurealm policies, procedures and practices related to the privacy of health information
4. Maintain all policies and procedures in written or electronic form

The contact information for the Privacy Official is as follows and subject to change

Kavitha Ayappan

Neurealm Private Ltd.,

E-mail: kavitha.ayappan@neurealm.com

b. Security Official

The company (Neurealm) has designated a Security Official to assist the Privacy Official and Privacy Coordinators in carrying out Neurealm adopted policies and procedures related to the privacy and security of individual's ePHI under HIPAA.

1. Responsibilities of the Security Official include :
2. Maintain ongoing communication with Privacy Official and all Privacy Coordinators
3. Assist in the development of policies and procedures of each covered functions related to the security of ePHI
4. Assist in the development and implementation of ongoing security awareness and training programs for the workforce of covered functions with respect to ePHI
5. Monitor the use of security measures to protect ePHIAssist in revising the Neurealm' policies and procedures related to privacy and security of ePHI as required to comply with changes in any applicable laws and document any changes.

The contact information for the Security Official is as follows and subject to change

Kavitha Ayappan

Neurealm Private Ltd.,

E-mail: kavitha.ayappan@neurealm.com

c. Privacy Coordinators

The company (Neurealm) has designated Privacy coordinators within each of the covered functions to assist the Privacy Official and the Security Officer in carrying out Neurealm adopted policies and procedures related to the privacy and security of PHI under HIPAA

Responsibilities of the Privacy Coordinators include:

1. Coordinate with Privacy Official and Security Official for maintaining ongoing communication
2. Develop and maintain procedures consistent with the policy for protection of PHI in the covered functions
3. Inform members of the covered functions about the policies and procedures through various mechanism, including staff meetings, orientation for new workforce members and ongoing education
4. Monitor the process for identifying workforce members within the covered functions who require access to PHI
5. Monitor compliance with the policies and procedures of the covered functions
6. Report to the Privacy Official and Security Official violations that result in an impermissible use of disclosure of ePHI
7. Help ensure compliance with HIPAA and Neurealm Policies and procedures

The Project Manager or Team Lead or Team Member as appointed by Delivery manager would play the role of Privacy Coordinator

d. Procedure

Project Manager shall update RACI Matrix to reflect who would play the role of Privacy coordinator

e. Applicable Regulations

45 C.F.R 164.530(a)

8. Records Retention

a. Policy

The company will maintain certain documentation regarding its HIPAA compliance in electronic form. Refer to Document Retention and Destruction Policy for the comprehensive list of documents for retention.

b. Procedure

Concerned functions must retain the following (but not limited) documentations for six years from the date of its creation or the date it was last in effect (whichever is later)

1. Policies and Procedures: - All policies and procedure documentation, including notice of privacy practices, approvals (if any)
2. Complaints: - The handling of any individual's complaints
3. Workforce Training: - The processes for and content of workforce training
4. Sanctions: - Handling of any sanctions against employee of its workforce who fail to comply with the HIPAA Policies
5. If state law requires longer retention periods, the state requirements should be adhered
6. All the requests and approvals emails shall be maintained as part of client's email repository folder for the transaction / queries related to PHI data or PII data handled by Neurealm employees

c. Applicable Regulations

45 C.F.R 164.530(j)

9. Research

a. Policy

As a policy Neurealm will not use or disclose PHI information for any research purpose

b. Procedure – Not Applicable

c. Applicable Regulations

45 C.F.R 164.501, 164.508, 164.512

10. Right to Request Access to Protected Health Information

a. Policy

Neurealm will not disclose PHI information to Individuals directly by any manner unless it is stated in the Business Associate Agreement.

b. Procedure

1) In case of any request received directly from individual, Neurealm covered function shall instruct the individual to approach covered entity

c. Applicable Regulations: 45 C.F.R 164.52

11. Right to Request an accounting of disclosures

a. Applicability – Not Applicable for the company (Neurealm) as the disclosure is maintained by covered entity
b. Policy
c. Procedure
d. Applicable Regulations
45 .F.R 164.528

12. Right to Request an amendment to PHI

a. Applicability – Not Applicable for the company (Neurealm) as the request to amendment to PHI is handled by covered entity
b. Policy
c. Procedure
d. Applicable Regulations
45 .F.R 164.526

13. Right to Request Confidential Communication

a. Applicability – Not Applicable for the company (Neurealm) as the request is handled by covered entity
b. Policy
c. Procedure
d. Applicable Regulations
45 C.F.R 164.522(b)

14. Right to Request restrictions on the use and disclosure of PHI

a. Applicability – Not Applicable for the company (Neurealm) as the request restrictions on the use and disclosure of PHI handled by covered entity
b. Policy
c. Procedure
d. Applicable Regulations
45 C.F.R 164.522(a)

15. Safeguarding PHI

a. Policy

Neurealm will implement appropriate administrative, technical, and physical safeguards in addition to Information Security Policies and Practices which will reasonably safeguard the confidentiality of protected health information. Designated covered functions may develop additional policies and procedures that are stricter than the attributes set forth below to maximize the privacy of protected health information

b. Procedure

1) Verbal Communications: - Do not disclose any PHI information verbally
2) Desktop and Working Area: Do not store any PHI information on the desktop and do not print it for any reasons. If there is a need to store PHI information for any processing, the entire folder / drive should be encrypted and decrypted accessible only by the authorized person
3) E-mails: - If there is a need for sending PHI information, it should be secured with a password or encryption
4) Computer Monitor: Position the computer monitor such that unauthorized person cannot view PHI and create password for screen savers
5) Storage: - If there is a need for storing e-PHI information in any form, ensure it is password protected or encrypted to prevent from unauthorized access

c. Applicable Regulations

45 C.F.R 164.530(c)

16. Training

a. Policy

Each designated covered function is responsible for training its workforce (including employees, contractors) with respect to the Neurealm's ISMS Policies, HIPAA policies, Fraud, Waste & Abuse and procedures on the use and disclosure of PHI as necessary and appropriate for the members of the workforce to carry out their function.

b. Procedure

1) It is responsibility of delivery manager to ensure that its workforce receives training on HIPAA and complete the assessment
2) Each employee who is working in Health Care projects shall complete the training no later than 14 April 2017. Each new employee must receive training within 30 days from the date of joining Neurealm or from the date the course is assigned to the employee for the annual refresher training
3) Any change in policy and procedures, the same shall be communicated within 30 days from after the change becomes effective
4) Neurealm Training function shall maintain all the records that the HIPAA training has been provided

c. Applicable Regulations

45 C.F.R 164.530 (b

17. Internal monitoring and auditing

a. Policy

All the projects that falls under covered function shall go through an independent audit by Quality function once in a quarter and audit findings shall be tracked to closure as per the agreed timeline.

b. Procedure

1) Prepare an annual audit plan with a mention of scope of HIPAA and other standard requirements to be covered in the scope
2) Quality functional shall prepare and send the audit schedule to auditees based on the audit plan
3) Quality function shall execute the audit as per the process and report the audit findings
4) Auditee shall respond to auditor with corrective action plan if any deficiencies (Non-compliance) reported. Auditee shall report the closure of audit findings
5) Audit team shall verify the closure of deficiencies / findings
6) For more detailed steps refer to the Process Management procedure for the Audit life cycle including the closure of audit findings.

c. Applicable Regulations

As per the OIG requirements

18. Reporting

a. Policy

All the projects that falls under covered function shall go through an independent audit by Quality function once in a quarter and audit findings shall be tracked to closure as per the agreed timeline.

b. Procedure

7) Follow the Process Management procedure for the Audit life cycle including the closure of audit findings.

c. Applicable Regulations

NA

VI. Reference

1. HIPAA Breach/ Risk Assessment Worksheet

Breach notification is required when (1) there has been a use/disclosure of protected health information (PHI) in violation of 45 CFR Subpart E, and (2) the covered entity/business associate cannot demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment (45 CFR 164.402).

Section 1 – Basic breach test		
If the answer to any of the questions in section 1 is "No" then - ☐ There is no breach • Stop the analysis, notification is not required • Document the case and provide appropriate training to the individuals involved		
No	Yes	
☐	☐	Did the use/disclosure violate the privacy rule? *(e.g. more than the minimum necessary; information was PHI; sent to unauthorized party; etc.)*
☐	☐	Did this use/disclosure involve unsecured PHI (not rendered unusable, unreadable, indecipherable)?
If the answer to all of the above questions in this section is "Yes", continue to section 2...		
Section 2 – Does an exception apply?		
If the answer to any of the questions in section 2 is "Yes" then – ☐ There is an exclusion • Stop the analysis, notification is not required • Document the case and provide appropriate training to the individuals involved		
Yes	No	
☐	☐	Was this an unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a CE or a BA, and was such acquisition, access, or use made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted?
☐	☐	Was this an inadvertent disclosure by a person who is authorized to access PHI at a CE/BA to another person authorized to access PHI at the same CE/BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted.

☐	☐	Is there a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information? If the answer to each of the above questions in this section is "No", proceed to section 3...

Section 3 – Is there a low probability that the PHI has been compromised?

Barring the exceptions in section 2 above, an impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of reidentification;
(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
(iii) Whether the protected health information was actually acquired or viewed; and (iv) The extent to which the risk to the protected health information has been mitigated.

These four factors along with any other factors relevant to the particular scenario should be taken together to determine if it can be demonstrated that the probability of compromise is low.

Yes	No	
☐	☐	Can it be demonstrated that there is a low probability that the PHI has been compromised based on the 4 factor risk assessment taken together with any other relevant factors?

If the answer to the above question is "No", then...

- Notification is required. For detailed requirements, see 45 CFR Subpart D: 164.404 Notification to individuals; 164.406 Notification to the media; 164.408 Notification to the Secretary, and 164.410 Notification by a business associate.
- Document the case and provide appropriate training to the individuals involved

Section 4 – Information of person completing the form

Name:	Title:
Signature:	Date:

2. Business Associate Decision Tree

Business Associate Decision Tree

This decision tree will help you determine if an entity is a "business associate" under HIPAA, as defined in 45 CFR § 160.103

Will an entity ("Entity") provide services to or on behalf of a Covered Entity? A "Covered Entity" is a healthcare provider or health plan, including most employee benefit plans.

[Note: This does not apply to (1) an employee, volunteer, trainee, or other person whose conduct is under the direct control of a Covered Entity (i.e., "workforce members"), (2) an Entity who is performing functions as part of a Covered Entity's organized health care arrangement,[1] or (3) Entities who receive info for their own purposes, and not to provide services to or on behalf of a Covered Entity (e.g., payors, government agencies, independent researchers, etc.).]

No → The Entity is not a business associate

Yes ↓

Will the Entity create, receive, maintain or transmit protected health info ("PHI") in the course of providing services to or on behalf of a Covered Entity?

[Note: This does not apply to Entities who may periodically see or hear PHI, but whose job duties for a Covered Entity do not involve the creation, receipt, maintenance, or transmission of PHI (e.g., a janitor, delivery person, or electrician who happens to be providing services in the building)].

No → The Entity is not a business associate

Yes ↓

Is the Entity a healthcare provider who is receiving the PHI for purposes of treating the individual?

Yes → The Entity is not a business associate

No ↓

Does the Entity perform a function or activity for the Covered Entity involving PHI that is regulated by HIPAA (e.g., healthcare operations or payment functions), including claims processing or administration; data analysis, processing or administration; or utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, or repricing services?

OR

Does the Entity provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services for a Covered Entity?

OR

Is the Entity a health information organization, e-prescribing gateway, or other Entity that provides data transmission services with respect to PHI and the Entity requires access to the PHI on a routine basis (i.e., the Entity is not merely the conduit for the PHI)?

OR

Does the outside entity person offer a personal health record to one or more individuals on behalf of a Covered Entity?

No → The Entity is not a business associate

Yes ↓

The Entity is a business associate. You must execute a valid business associate agreement with the Entity before disclosing PHI to the Entity. The business associate agreement must contain the elements in 45 CFR §§ 164.314(a) and 164.504(e)