

# HIPAA Manual

## HIPAA Policies and Procedures: Instructions and Confirmation

This document contains instructions for creating your pharmacy's HIPAA Policies and Procedures Manual. After confirming that you have read and understand the process, you will then be able to fill out a form that will be used to create your Manual.

1. After reading these instructions, check the box to the left of "I have read and understand the instructions and will now fill out the form." This will be the attestation that you have read the instructions and filled out the form to create your HIPAA Policies and Procedures Manual Policy Form.
2. Fill in all the blanks that apply to your operation (location, compliance officer, etc.). This information will populate to the appropriate places throughout the document on page 3.
3. When you are confident that all pertinent information has been filled out in the form, click "**FILE**" then "**SAVE AS**". This will start the process of creating your HIPAA Policies and Procedures Manual. **(Caution: this could take 2 to 5 minutes—please be patient).**
4. After saving your manual, click on the "**Print**" button at the top and print out your customized HIPAA Manual. **(Caution: the document is 110 pages long—so be sure you have plenty of paper in your printer).**

I have read and understand the instructions and will now fill out the form.

## **\_\_\_\_\_ HIPAA MANUAL**

Disclaimer: This HIPAA Manual is intended to serve as a guide to implementing effective HIPAA policies and procedures. Each pharmacy will need to adapt this Manual to fit its specific staffing, technology, and operational needs. The policies, procedures and staff training described in this Manual must be customized, incorporated into \_\_\_\_\_'S daily operations and approved and disseminated to staff and others that have access to HIPAA protected information in order to comply with HIPAA regulations and applicable 3<sup>rd</sup> party payor contractual obligations. Arete does not make any warranties regarding the completeness, accuracy or reliability of the information contained within this Manual. Any action you take based upon the information contained herein is strictly at your own risk, and Arete will not be liable for any losses and/or damages in connection with the use of this Manual.

Disclaimer: This Manual is intended for internal use only. Any unauthorized copying, alteration, distribution, transmission, performance, display or other use of this material – other than for the purpose stated herein – is expressly prohibited.

# HIPAA Manual

Please fill in the fields below to auto-populate (customize) your HIPAA Policy with the information that relates to the administrative roles and responsibilities for this manual.

Pharmacy Name:

NCPDP Number:

Pharmacy Address:

Pharmacy City:

Pharmacy State:

Pharmacy Zip Code:

Pharmacy Manager Name (First, Last):

Pharmacy Manager Phone:

Pharmacy Manager Email:

Security Officer Name (First, Last):

Security Officer Phone:

Security Officer Email:

Privacy Officer Name (First, Last)

Privacy Officer Phone:

Privacy Officer Email:

Pharmacy Regional Manager Name (First, Last) \*:

*Optional: only complete if your pharmacy is a chain that has upper regional management*

Pharmacy Regional Manager Phone

Pharmacy Regional Manager Email

Compliance Hotline Number

Owner Name:

Approval Date:

Effective Date:

## HIPPA Policies and Procedures

### Overview

This Manual is intended to ensure that \_\_\_\_\_ is compliant with the standards, requirements, and implementation specifications of the Health Insurance Portability and Accountability Act of 1996, and the regulations set forth at 45 CFR Part 160 and Part 164, as amended by the Health Information Technology for Economic and Clinical Health Act (collectively, “**HIPAA**”). The main purpose of HIPAA is to help consumers maintain their health coverage, but the Act also includes a separate set of provisions called **Administrative Simplification Provisions**, which are aimed at improving the efficiency and effectiveness of the health care system. These provisions were also established to create a national standard for safeguarding the privacy and security of **Protected Health Information (PHI)**. HIPAA preempts contrary provisions of State law unless such provisions are more stringent than the HIPAA privacy standard.

Under HIPAA, an entity or individual must comply with the terms set forth therein if it constitutes a covered entity or a Business Associate (BA), or subcontractor of the business with whom the business associate shares individually identifiable health information (IHH) or PHI. Generally speaking, covered entities fall into one of three categories: healthcare providers, health plans, and healthcare clearinghouses.

\_\_\_\_\_ is bound to comply with HIPAA because it is a healthcare provider, and thus meets the definition of a covered entity. Additionally, if \_\_\_\_\_ provides services to a covered entity that involve the use or disclosure of PHI then \_\_\_\_\_ will be deemed a business associate under HIPAA. Accordingly, \_\_\_\_\_ has adopted the following Policies and Procedures (collectively, this “**Policy**”) to ensure that its business, Workforce Members (staff, volunteers, trainees, vendors, contractors, consultants, agents, and other persons whose conduct on behalf of \_\_\_\_\_), and business associates remain HIPAA compliant when performing work on behalf of pharmacy. Unless specifically stated otherwise, all policies and procedures stated herein apply to all Workforce Members, Business Associates, and all others who have access to or work with \_\_\_\_\_’S PHI.

### Emergency Contact Information

When faced with an emergency that encompasses the material covered by this Manual, Workforce Member shall contact the appropriate person in an effort to resolve the situation. In so doing, Workforce Member shall keep in mind the following hierarchy of command and make best efforts to reach the appropriate person. Workforce Member shall first notify his/her immediate supervisor, and if unavailable, Workforce Member shall then make an effort to notify the Privacy Officer. When reporting an emergency situation, the Workforce Member shall make an effort to be cognizant of all pertinent facts, and shall report these facts up the chain of command. An example of pertinent facts includes: the nature of the emergency, the number and types of records involved, and the steps that have been taken to mitigate the breach of PHI.

## Local Contact Information

Privacy Officer Name:

Privacy Officer Primary Phone Number:

Privacy Officer Secondary Phone Number:

Privacy Officer Email:

Manager Name:

Manager Phone Number

Manager Secondary Phone Number:

Manager Email:

## Health and Human Services (HHS) Contact Information

For direct media inquiries please contact the HHS Press Office at (202) 690-6343.

For questions pertaining to Health Information Privacy or Patient Safety, email [OCRPrivacy@hhs.gov](mailto:OCRPrivacy@hhs.gov).

To report a breach of unsecured PHI, use the following URL:  
[https://ocrportal.hhs.gov/ocr/breach/wizard\\_breach.jsf?faces-redirect=true](https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true)

Should you need assistance pertaining to the above URL/website or have any questions regarding any information contained therein, please email [OCRPrivacy@hhs.gov](mailto:OCRPrivacy@hhs.gov) or call toll-free: (800) 368-1019; TDD toll-free: (800) 537-7697

The above website can be utilized to electronically submit a breach report form. **If a breach of unsecured protected health information affects 500 or more individuals of a State of jurisdiction**, a covered entity must notify the Secretary of the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach. The covered entity must submit the notice electronically by clicking on the link below and completing all of the required fields of the breach notification form.

**If a breach of unsecured protected health information affects fewer than 500 individuals of a State or jurisdiction**, a covered entity must notify the Secretary of the breach within 60 days of the end of the calendar year in which the breach was discovered. (A covered entity is not required to wait until the end of the calendar year to report breaches affecting fewer than 500 individuals; a covered entity may report such breaches at the time they are discovered.) The covered entity may report all of its breaches affecting fewer than 500 individuals on one date, but the covered entity must complete a separate notice for each breach incident. Please refer to the Breach Notification Policy for additional information.

If a covered entity discovers additional information that supplements, modifies, or clarifies a previously submitted notice to the Secretary, it may submit an additional form by checking the appropriate box to indicate that it is an addendum to the initial report, using the transaction number provided after its submission of the initial breach report.

For non-privacy related inquiries, including comments or questions about OCR's web site, email [OCRMail@hhs.gov](mailto:OCRMail@hhs.gov) or write to:

**Office for Civil Rights**

U.S. Department of Health and Human Services  
200 Independence Avenue, SW  
Room 509F, HHH Building  
Washington, D.C. 20201  
Toll-free: (800) 368-1019; TDD toll-free: (800) 537-7697

**Eastern and Caribbean Region - (New Jersey, New York, Puerto Rico, Virgin Islands)**

Office for Civil Rights U.S. Department of Health and Human Services, Jacob Javits Federal Building  
26 Federal Plaza - Suite 3312  
New York, NY 10278  
Customer Response Center: (800) 368-1019 Fax: (202) 619-3818 TDD: (800) 537-7697  
Email: [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

**Kansas City**

Office for Civil Rights - U.S. Department of Health and Human Services  
601 East 12th Street - Room 353  
Kansas City, MO 64106  
Customer Response Center: (800) 368-1019; Fax: (202) 619-3818; TDD: (800) 537-7697  
Email: [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

**Mid-Atlantic Region - (Delaware, District of Columbia, Maryland, Pennsylvania, Virginia, West Virginia)**

Office for Civil Rights U.S. Department of Health and Human Services  
150 S. Independence Mall West, Suite 372, Public Ledger Building  
Philadelphia, PA 19106-9111  
Customer Response Center: (800) 368-1019 Fax: (202) 619-3818 TDD: (800) 537-7697  
Email: [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

**Midwest Region - (Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, Ohio, Wisconsin)**

Office for Civil Rights U.S. Department of Health and Human Services  
233 N. Michigan Ave., Suite 240  
Chicago, IL 60601  
Customer Response Center: (800) 368-1019; Fax: (202) 619-3818; TDD: (800) 537-7697  
Email: [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

**New England Region - (Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont)**

Office for Civil Rights U.S. Department of Health and Human Services Government Center  
J.F. Kennedy Federal Building - Room 1875  
Boston, MA 02203  
Customer Response Center: (800) 368-1019 Fax: (202) 619-3818 TDD: (800) 537-7697  
Email: [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

**Pacific Region - (Alaska, American Samoa, Arizona, California, Commonwealth of the Northern Mariana Islands, Federated States of Micronesia, Guam, Hawaii, Idaho, Marshall Islands, Nevada, Oregon, Republic of Palau, Washington)**

Office for Civil Rights U.S. Department of Health and Human Services

90 7th Street, Suite 4-100

San Francisco, CA 94103

Customer Response Center: (800) 368-1019; Fax: (202) 619-3818; TDD: (800) 537-7697

Email: [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

**Rocky Mountain Region - (Colorado, Montana, North Dakota, South Dakota, Utah, Wyoming)**

HHS/Office for Civil Rights

1961 Stout Street Room 08-148

Denver, CO 80294

Customer Response Center: (800) 368-1019; Fax: (202) 619-3818; TDD: (800) 537-7697

Email: [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

**Southeast Region - Atlanta (Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, Tennessee)**

Office for Civil Rights U.S. Department of Health and Human Services

Sam Nunn Atlanta Federal Center, Suite 16T70

61 Forsyth Street, S.W.

Atlanta, GA 30303-8909

Customer Response Center: (800) 368-1019 Fax: (202) 619-3818

**Southwest Region - (Arkansas, Louisiana, New Mexico, Oklahoma, Texas)**

Office for Civil Rights - U.S. Department of Health and Human Services

1301 Young Street, Suite 1169

Dallas, TX 75202

Customer Response Center: (800) 368-1019; Fax: (202) 619-3818; TDD: (800) 537-7697

Email: [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

To help \_\_\_\_\_ prepare for a HIPAA related audit, please consult the following website for a list of criteria that OCR will use to assess your pharmacy:

<https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html>

## HIPAA Personnel Designation Policy

---

### I. PURPOSE AND APPLICABILITY

HIPAA requires the appointment of a Privacy Officer, Security Officer, and Designated Person/Office Contact. While such appointments are required, there is nothing that bars a single individual from fulfilling all of the roles. HIPAA is cognizant of the fact that covered entities, such as pharmacies, come in various different sizes and that consequently, what might be practical or advantageous for one pharmacy might be prohibitive for another. Consequently, this Policy is designed to be flexible regarding the appointment of said positions. Please review a description of the job responsibilities for these roles below and then complete the accompanying designation forms as your \_\_\_\_\_ best sees fit.

The appointment of a Privacy Officer is required under HIPAA §164.308(a)(2)(i). This person is to be, "... responsible for the development and implementation of the policies and procedures of the entity." In other words, the Privacy Officer is responsible for the entity's entire HIPAA compliance program. In contrast, the role of the Security Officer under HIPAA §164.308(a)(2) is to be, "... responsible for the development and implementation of the policies and procedures," required under Subpart C of Part 164, i.e., the Security Rule. HIPAA also requires the appointment of a Designated Person/Office Contact under §164.530(a)(1)(ii). The Designated Person/Office Contact is responsible for receiving HIPAA complaints, and providing information pertaining to \_\_\_\_\_'S privacy notices.

\_\_\_\_\_ is responsible for complying with this Policy.

### II. DETAILED POLICY STATEMENT

#### Requirements

1. \_\_\_\_\_ must appoint a Privacy Officer, a Security Officer, and a Designated Person/Office Contact. Nothing prohibits one person from serving all three roles.
2. The role of the Privacy officer is to take responsibility for the development and implementation of \_\_\_\_\_'S entire HIPAA compliance program.
3. The role of the Security Officer is to take responsibility for the development and implementation of \_\_\_\_\_'S policies and procedures under the Security Rule.
4. The Designated Person/Office Contact is responsible for receiving HIPAA complaints and providing further information regarding the matters of notice addressed under HIPAA §164.520.
5. \_\_\_\_\_ will make an immediate effort to fill these positions in the event that any one of them becomes vacant.



### **III. RESPONSIBILITY**

1. \_\_\_\_\_ is responsible for complying with this Policy.
2. In the event that \_\_\_\_\_ works with a Business Associate, the Business Associate must have substantially similar policies and procedures in place, and those procedures must satisfy all of the requirements expressed under the Security Rule.
3. This Policy is to be implemented and maintained by the Privacy Officer.

### **IV. DOCUMENTATION**

1. \_\_\_\_\_ must maintain written documentation (which may be electronic) of these designations.
2. \_\_\_\_\_ must retain the documentation for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

### **V. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_.

\_\_\_\_\_ **'S Designated Privacy Officer**

The following individual has been designated as the Privacy Officer for \_\_\_\_\_.

\_\_\_\_\_  
Privacy Officer

The Privacy Officer is responsible for overseeing the development, implementation and maintenance of the \_\_\_\_\_'S HIPAA Compliance Program. A non-exhaustive list of the responsibilities under this role includes:

- Working with the Security Officer, Management and Ownership to create and implement the Policies and Procedures to comply with the Privacy, Security and Breach Rules
- Managing all facets of the HIPAA Compliance Program
- Ensuring all employees are appropriately trained on the HIPAA Regulations and \_\_\_\_\_'S HIPAA Policies and Procedures
- Monitoring access to PHI
- Performing ongoing assessments of the HIPAA Compliance Program
- Working with legal counsel to address HIPAA concerns
- Conduct ongoing HIPAA compliance monitoring activities
- Establish, with management, operations and Security Officer, a mechanism to track access to PHI, and allow qualified individuals to review or receive a report on such activity.
- Work cooperatively with other key workforce members, including Business Associates, in overseeing client rights to inspect and amend PHI as appropriate and restrict access to PHI when appropriate.
- Work with the Security Officer, Contact Person (or office), Corporate Compliance Officer, Director of Human Resources and/or legal counsel to establish a process for receiving, documenting, tracking, investigating, and taking corrective action on all complaints concerning \_\_\_\_\_'s privacy policies and procedures.
- Implement consistent application of sanctions to all individuals in \_\_\_\_\_'s workforce, and for all Business Associates in cooperation with the Security Officer, Human Resources Department, administration, and/or legal counsel.
- In collaboration with legal counsel, identify Business Associates that receive PHI and review existing contracts with these entities for compliance with HIPAA.

- Review and evaluate proposed business contracts and other documents to identify and correct potential conflicts between \_\_\_\_\_'S privacy policies and procedures and applicable federal and state laws and regulations.

  
\_\_\_\_\_  
Privacy Officer's Signature

\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Owner's Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Owner's Printed Name

\_\_\_\_\_  
Title

\_\_\_\_\_’S Designated Security Officer

The following individual has been designated as the Security Officer for \_\_\_\_\_.



\_\_\_\_\_  
Security Officer

The Security Officer (“SO”) is responsible for overseeing the development, implementation and maintenance of the \_\_\_\_\_’S HIPAA Compliance Program as it pertains to the Security Rule. In order to fulfill its responsibilities, SO may collaborate with \_\_\_\_\_’S Compliance Officer, Privacy Officer, legal counsel, and/or any other person whom the SO, in his or her sole discretion, deems prudent to consult. A non-exhaustive list of the responsibilities under this role includes:

- Working with the Privacy Officer, Management and Ownership to create and Implement the Policies and Procedures to comply with the Security Rule
- Conducting Risk Analyses
- Creating and testing a Disaster Recovery/Contingency Plan
- Continually evaluating \_\_\_\_\_’S security systems and potential threats
- Ensuring employees are appropriately trained on proper use of \_\_\_\_\_’S Electronic Systems
- Monitoring access to e-PHI
- Issuing access authorization
- Modifying or terminating access authorization as positions change
- Password management
- Overseeing data backup and access to data during emergencies
- Preventing, detecting, and mitigating viruses
- Reviewing technical controls such as the adequacy of firewalls
- Overseeing the security training of Workforce members
- Overseeing security breach and security Incident responses

   
\_\_\_\_\_  
Security Officer's Signature

\_\_\_\_\_  
Date

   
\_\_\_\_\_  
Owner's Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Owner's Printed Name

\_\_\_\_\_  
Title

The following individual has been designated as the Contact Person for \_\_\_\_\_.

\_\_\_\_\_  
Designated Contact Person/Office

The Contact Person/Office is responsible for receiving complaints and providing information related to the Notice of Privacy Practices.

   
\_\_\_\_\_  
Contact Person's Signature (If applicable)

\_\_\_\_\_  
Date

   
\_\_\_\_\_  
Owner's Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Owner's Printed Name

\_\_\_\_\_  
Title

## HIPAA Privacy Rule Notice Policy

---

### I. PURPOSE AND APPLICABILITY

The HIPAA Privacy Rule grants the patient or their representative several rights. Among these rights are the right to adequate notice regarding the various ways that a Covered Entity might use or disclose a patient's PHI. Additionally, the patient or their representative has the right to know what privacy rights the patient has regarding his/her PHI, as well as the legal duties that a Covered Entity has with respect to PHI. For reasons explained in the Preface Section of this Policy, \_\_\_\_\_, its Workforce, Business Associates, and all others who have access to \_\_\_\_\_'S PHI are required to comply with the Privacy Rule. Consequently, under HIPAA Section 164.520 \_\_\_\_\_ is required to provide patients with notice (in paper or electronic form) of these rights. This Policy Section 4 addresses the notice component of the Privacy Rule and is designed to ensure that \_\_\_\_\_'s notice document/s meet the requirements articulated under HIPAA.

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.

### II. DETAILED POLICY STATEMENT

#### Requirements: Privacy Rule Notice

1. HIPAA requires that notice of \_\_\_\_\_'S privacy practices be made available to all customers and must conform with the following requirements:
2. \_\_\_\_\_ must post the "privacy notice" (the Notice) in a clear and prominent location where it is reasonable to expect individuals seeking service from \_\_\_\_\_ to be able to read it. Some examples of appropriate places to post the Notice include: \_\_\_\_\_'S entrance door, drop-off window, and/or drug counter.
3. \_\_\_\_\_ must make a copy of its notice available to any individual who requests it, irrespective of whether such individual is seeking the services of \_\_\_\_\_.
4. If \_\_\_\_\_ has a direct treatment relationship with the individual then it must provide the Notice no later than the date of the first service delivery, including service delivered electronically. However, in an emergency situation, \_\_\_\_\_ is permitted to give the individual the Notice as soon as reasonably practicable after the emergency situation.
5. Except in an emergency treatment situation, \_\_\_\_\_ must always make a good faith effort to obtain a written acknowledgement of receipt of the Notice provided to an individual that has a direct treatment relationship with \_\_\_\_\_. If \_\_\_\_\_ cannot obtain a written acknowledgement of receipt for such an individual, then it must document its good faith efforts to do so, and the reasons why the acknowledgement was not obtained.

6. In the event that \_\_\_\_\_ has a website, then it must post the Notice to its website, and it must make the Notice available electronically through its website.
7. \_\_\_\_\_ may provide the Notice as required, to an individual via email, provided the individual has consented to receiving an electronic copy and such consent has not been withdrawn. If \_\_\_\_\_ knows that the email transmission has failed then it must provide a paper copy of the Notice to the individual.
8. If the first service delivery to an individual occurs in electronic form, then \_\_\_\_\_ must provide electronic Notice automatically and contemporaneously in response to the individual's first request for service.

#### **Privacy Rule Notice: General Content Requirements**

The content of the notice must contain the following elements:

1. \_\_\_\_\_ must provide a notice that is written in plain language and that clearly explains how \_\_\_\_\_ may use and disclose PHI.
2. The notice must contain the following statement as a header or otherwise be prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."
3. A description, including at least one example, of the types and uses of disclosure that \_\_\_\_\_ is permitted to make for each of the following purposes: treatment, payment, and healthcare operations.
4. A description of each of the other purposes for which a \_\_\_\_\_ is permitted or required to use PHI without the individual's written authorization.
5. The description must include sufficient detail to put the individual on notice of the uses and disclosures that are permitted or required by the privacy regulations and other applicable laws.
6. If the use or disclosure of PHI is materially limited by other applicable law, then such use or disclosure must reflect the more stringent law.
7. A description of the types of uses and disclosures of PHI that require the individual's written authorization under HIPAA section 164.508(a)(2)-(a)(4), which relates generally to psychotherapy notes, marketing practices, and the sale of PHI, and a statement that the individual may revoke an authorization as provided by § 164.508(b)(5).

#### **Privacy Rule Notice: Content Requirements for Individual Rights**

Regarding individual rights, the notice must contain statements that address the following:

1. The notice must address the individual's rights with respect to PHI and a description of how the individual may exercise these rights.
2. The notice must make clear that the individual has the right to request restrictions on the use and disclosures of his/her PHI, and \_\_\_\_\_ must permit the individual to exercise this right.



3. The notice must make known that \_\_\_\_\_ is not obligated to comply with such a request under section (II)(3.2) of this Policy unless required to do so under HIPAA section 164.522(a)(1)(iv) which involves instances where \_\_\_\_\_ has already agreed to restrict an individual's PHI, but must then make a disclosure of said PHI so that the individual in question can receive emergency treatment.
4. The notice must make the individual aware that he/she has the right to receive confidential communications regarding PHI.
5. The right of the individual to inspect and/or obtain a copy PHI, as well as to direct \_\_\_\_\_ to transmit a copy to a designated person or entity of the individual's choice. The individual also has the right to request that the PHI be delivered in a particular manner. For example, the patient may ask that a hardcopy be mailed or that a soft copy be faxed or emailed. Where possible, \_\_\_\_\_ should accommodate such requests.
6. The right of the individual to request an amendment of PHI.
7. The individual's right to request an accounting of his/her PHI.
8. The right of the individual to obtain a paper copy of the notice from \_\_\_\_\_ upon request. The individual also has the right to request that the PHI be delivered in a particular manner (i.e., fax, mail, etc.).
9. Finally, the notice must make clear that an individual has the right to access their PHI in a designated record set.

A record means any item, collection, or grouping of information that (1) includes PHI and (2) is maintained, collected, used, or disseminated by or for a CE.

A designated record set is comprised of the following types of information:

- Enrollment, payment, claims adjudication, and medical management records maintained by or for a health plan;
- Medical records and billing records about individuals that are maintained by a physician or other provider; and
- Records used, in whole or in part, by a CE to make decisions about individuals

In addition, HHS has made clear that records that otherwise meet the definition of a designated record set, and which are held by a CE's business associate, are part of the CE's designated record set.

**Privacy Rule Notice: \_\_\_\_\_'S Duties**

The notice must contain the following statements regarding \_\_\_\_\_'S duties:

1. A statement that \_\_\_\_\_ is required by law to maintain the privacy of PHI, to provide individuals with notice of its legal duties and privacy practices with respect to PHI, and to notify affected individuals following a breach of unsecured PHI.
2. A statement that \_\_\_\_\_ is required to abide by the terms of the notice currently in effect.

3. A statement that \_\_\_\_\_ reserves the right to implement revisions to its privacy practices and that such changes might impact all PHI, including previously obtained PHI which \_\_\_\_\_ maintains. Such a statement must also include an explanation as to how \_\_\_\_\_ will provide the revised notice to its customers.
4. The notice must contain a statement that individuals may complain to \_\_\_\_\_ or the Secretary of Health & Human Services (HHS) if they believe their privacy rights have been violated, a description of how the individual may file a complaint with the \_\_\_\_\_, and a statement that the individual will not be retaliated against for filing such a statement.
5. \_\_\_\_\_ must provide in the notice, the name, or title, and telephone number of a person or office that individuals can contact to receive additional information.
6. The notice must contain an effective date. Such date may not be earlier than the date on which the notice is printed or otherwise published.
7. \_\_\_\_\_ must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the \_\_\_\_\_'S legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the Notice in which such material change is reflected.

#### **Privacy Rule Notice: Notice Requiring Separate Statements**

The Notice must include separate statements where \_\_\_\_\_ plans to engage in the following activity:

\_\_\_\_\_ contacts the individual in an effort to raise funds for \_\_\_\_\_. Where \_\_\_\_\_ does so, the separate statement must also make clear that the individual has the right to opt out.

### **III. RESPONSIBILITY**

1. All Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. This Policy is to be implemented and maintained by the Privacy Officer.

### **IV. DOCUMENTATION**

1. \_\_\_\_\_ must maintain copies of the Notice (original and revisions), written acknowledgements of receipt, and all documentation pertaining to good faith efforts to obtain acknowledgement receipts, for a period of six (6) years from the date that such documents were last in effect.

### **V. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_.

## **SAMPLE NOTICE OF PRIVACY PRACTICES**

### **Your Information. Your Rights. Our Responsibilities.**

---

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

#### **LAYERED SUMMARY TEXT –**

#### **Your Rights**

You have the right to:

- Receive a copy of your paper or electronic medical record
- Correct your paper or electronic medical record
- Request confidential communication
- Ask us to limit the information we share
- Receive a list of those with whom we've shared your information
- Receive a copy of this privacy notice
- Choose someone to act for you
- File a complaint if you believe your privacy rights have been violated

#### **Your Choices**

You have some choices in the way that we use and share information as we:

- Tell family and friends about your condition
- Provide disaster relief
- Include you in a hospital directory
- Provide mental health care
- Market our services and sell your information
- Raise funds

#### **Our Uses and Disclosures**

We may use and share your information as we:

- Treat you
- Run our organization
- Bill for your services
- Help with public health and safety issues

- Do research
- Comply with the law
- Respond to organ and tissue donation requests
- Work with a medical examiner or funeral director
- Address workers' compensation, law enforcement, and other government requests
- Respond to lawsuits and legal actions

## **Your Rights**

**When it comes to your health information, you have certain rights.** This section explains your rights and some of our responsibilities to help you.

### **Get an electronic or paper copy of your medical record**

- You can ask to see or get an electronic or paper copy of your medical record and other health information we have about you. Ask us how to do this.
- We will provide a copy or a summary of your health information, usually within 30 days of your request. We may charge a reasonable, cost-based fee.

### **Ask us to correct your medical record**

- You can ask us to correct health information about you that you think is incorrect or incomplete. Ask us how to do this.
- We may say "no" to your request, but we'll tell you why in writing within 60 days.

### **Request confidential communications**

- You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address.
- We will say "yes" to all reasonable requests.

### **Ask us to limit what we use or share**

- You can ask us not to use or share certain health information for treatment, payment, or our operations. We are not required to agree to your request, and we may say "no" if it would affect your care.
- If you pay for a service or health care item out-of-pocket in full, you can ask us not to share that information for the purpose of payment or our operations with your health insurer. We will say "yes" unless a law requires us to share that information.

### **Get a list of those with whom we've shared information**

- You can ask for a list (accounting) of the times we've shared your health information for six years prior to the date you ask, who we shared it with, and why.
- We will include all the disclosures except for those about treatment, payment, and health care operations, and certain other disclosures (such as any you asked us to make). We'll

provide one accounting a year for free but will charge a reasonable, cost-based fee if you ask for another one within 12 months.

### **Get a copy of this privacy notice**

You can ask for a paper copy of this notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy promptly.

### **Choose someone to act for you**

- If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information.
  - We will make sure the person has this authority and can act for you before we take any action.

### **File a complaint if you feel your rights are violated**

- You can complain if you feel we have violated your rights by contacting us using the information on page 1.
- You can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting [www.hhs.gov/ocr/privacy/hipaa/complaints/](http://www.hhs.gov/ocr/privacy/hipaa/complaints/).
- We will not retaliate against you for filing a complaint.

### **Your Choices**

**For certain health information, you can tell us your choices about what we share.** If you have a clear preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions.

In these cases, you have both the right and choice to tell us to:

- Share information with your family, close friends, or others involved in your care
- Share information in a disaster relief situation
- Include your information in a hospital directory

*If you are not able to tell us your preference, for example if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.*

In these cases, we never share your information unless you give us written permission:

- Marketing purposes
- Sale of your information
- Most sharing of psychotherapy notes

In the case of fundraising:

- We may contact you for fundraising efforts, but you can tell us not to contact you again.

## **Our Uses and Disclosures**

### **How do we typically use or share your health information?**

We typically use or share your health information in the following ways.

#### **Treat you**

We can use your health information and share it with other professionals who are treating you.

*Example: A doctor treating you for an injury asks another doctor about your overall health condition.*

#### **Run our organization**

We can use and share your health information to run our practice, improve your care, and contact you when necessary.

*Example: We use health information about you to manage your treatment and services.*

#### **Bill for your services**

We can use and share your health information to bill and get payment from health plans or other entities.

*Example: We give information about you to your health insurance plan so it will pay for your services.*

### **How else can we use or share your health information?**

We are allowed or required to share your information in other ways – usually in ways that contribute to the public good, such as public health and research. We have to meet many conditions in the law before we can share your information for these purposes. For more information see: [www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html](http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html).

#### **Help with public health and safety issues**

We can share health information about you for certain situations such as:

- Preventing disease
- Helping with product recalls
- Reporting adverse reactions to medications
- Reporting suspected abuse, neglect, or domestic violence
- Preventing or reducing a serious threat to anyone's health or safety

## **Do research**

We can use or share your information for health research.

## **Comply with the law**

We will share information about you if state or federal laws require it, including with the Department of Health and Human Services if it wants to see that we're complying with federal privacy law.

## **Respond to organ and tissue donation requests**

We can share health information about you with organ procurement organizations.

## **Work with a medical examiner or funeral director**

We can share health information with a coroner, medical examiner, or funeral director when an individual die.

## **Address workers' compensation, law enforcement, and other government requests**

We can use or share health information about you:

- For workers' compensation claims
- For law enforcement purposes or with a law enforcement official
- With health oversight agencies for activities authorized by law
- For special government functions such as military, national security, and presidential protective services

## **Respond to lawsuits and legal actions**

We can share health information about you in response to a court or administrative order, or in response to a subpoena.

## **Our Responsibilities**

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.

For more information see:

[www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html](http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html).

## Changes to the Terms of this Notice

**We can change the terms of this notice, and the changes will apply to all information we have about you. The new notice will be available upon request, in our office, and on our web site.**

## Other Instructions for Notice

- Insert Effective Date of this Notice
- Insert name or title of the privacy official (or other privacy contact) and his/her email address and phone number.
- Insert any special notes that apply to your entity's practices such as "we never market or sell personal information."
- The Privacy Rule requires you to describe any state or other laws that require greater limits on disclosures. For example, "We will never share any substance abuse treatment records without your written permission." Insert this type of information here. If no laws with greater limits apply to your entity, no information needs to be added.
- If your entity provides patients with access to their health information via the Blue Button protocol, you may want to insert a reference to it here.
- If your entity is part of an OHCA (organized health care arrangement) that has agreed to a joint notice, use this space to inform your patients of how you share information within the OHCA (such as for treatment, payment, and operations related to the OHCA). Also, describe the other entities covered by this notice and their service locations. For example, "This notice applies to Grace Community Hospitals and Emergency Services Incorporated which operate the emergency services within all Grace hospitals in the greater Dayton area."



## HIPAA Limited Data Set

---

### I. PURPOSE AND APPLICABILITY

HIPAA §164.514(e)(1) permits \_\_\_\_\_ to use or disclose limited data sets. Accordingly, the purpose of this Policy is to ensure that \_\_\_\_\_ has the proper procedures in place to handle such actions.

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.

### II. DETAILED POLICY STATEMENT

1. A limited data set is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:
  - i. Names;
  - ii. Postal address information, other than town or city, State, and zip code;
  - iii. Telephone numbers;
  - iv. Fax numbers;
  - v. Electronic mail addresses;
  - vi. Social security numbers;
  - vii. Medical record numbers;
  - viii. Health plan beneficiary numbers;
  - ix. Account numbers;
  - x. Certificate/license numbers;
  - xi. Vehicle identifiers and serial numbers, including license plate numbers;
  - xii. Device identifiers and serial numbers;
  - xiii. Web Universal Resource Locators (URLs);
  - xiv. Internet Protocol (IP) address numbers;
  - xv. Biometric identifiers, including finger and voice prints; and
  - xvi. Full face photographic images and any comparable images.
2. \_\_\_\_\_ may use or disclose a limited data in instances in which a permissible use or disclosure of PHI exists, for research purposes, public health, or health care operations.
3. \_\_\_\_\_ may disclose a limited data set to a 3rd party contractor only if \_\_\_\_\_ obtains satisfactory assurance in the form of a data use agreement that the limited data set recipient will only use or disclose the PHI for limited purposes.
4. A data use agreement must contain the following:
  - Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or

further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;

- Establish who is permitted to use or receive the limited data set; and
  - Provide that the limited data set recipient will:
    - Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
    - Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
    - Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
    - Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
  - Not identify the information or contact the individuals.
5. \_\_\_\_\_ may hire a business associate to create a limited data set. To do so, \_\_\_\_\_ must enter into a business associate agreement with the 3rd party.
6. Only the PO or his/her designee shall have authority to comply with requests to use or disclose limited data sets. Further, where a data agreement or business associate agreement is required, \_\_\_\_\_'S PO shall be responsible for reviewing and approving the agreement.
7. If \_\_\_\_\_ receives a limited data set from a covered entity then it will use and/or disclose said data in accord with all applicable laws and the terms of the applicable data use agreement.

### **III. RESPONSIBILITY**

1. This Policy applies to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.
2. This Policy is to be implemented and maintained by the Privacy Officer.

### **IV. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_.

## HIPAA Designated Record Set

---

### I. PURPOSE AND APPLICABILITY

HIPAA allows a patient, or their designated representative, the right to access portions of their medical record, known as a “designated record set,” for the purpose of obtaining copies or amending their PHI. Accordingly, the purpose of this Policy is to ensure that \_\_\_\_\_ has the proper procedures in place to handle such requests.

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.

### II. DETAILED POLICY STATEMENT

1. HIPAA §164.501 defines a designated record set as: A record means any item, collection, or grouping of information that (1) includes PHI and (2) is maintained, collected, used, or disseminated by or for a CE.
2. A designated record set is comprised of the following types of information:
  - Enrollment, payment, claims adjudication, and medical management records maintained by or for a health plan;
  - Medical records and billing records about individuals that are maintained by a physician or other provider; and
  - Records used, in whole or in part, by a CE to make decisions about individuals
3. Individual patients of \_\_\_\_\_ do not have the right to obtain or amend information that is not contained within the designated record set. For example, if a patient calls in to ask a pharmacist a question, the information that the pharmacist learns about the patient through that interaction would not be subject to a request for access or amendment unless the information was recorded in the designated record set. Further, HIPAA does not grant patients the right to access psychotherapy notes, information that has been compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative proceeding, or PHI that is held by clinical laboratories when the Clinical Laboratory Improvements Amendments of 1988 (CLIA) expressly prohibits such access or when PHI is held by certain laboratories that are not subject to regulation under CLIA. Finally, certain instances exist in which an individual's request to access or amend a designated record set can be denied. Workforce Members should consult the PO to learn more about this.
4. In addition to the above, information which is created, collected, or maintained by \_\_\_\_\_ for purposes which do not include decision making about the patient and/or which is exempt from disclosure to the individual, are types of information which fall outside the scope of the designated record set. \_\_\_\_\_'S employee records -including health records – are also not the type of information that can be contained in a designated record set.

5. Only \_\_\_\_\_'S PO or his/her designee is authorized on behalf of \_\_\_\_\_ to determine whether a particular piece of information is subject to inclusion in a designated record set.

### **III. RESPONSIBILITY**

1. This Policy applies to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.
2. This Policy is to be implemented and maintained by the Privacy Officer.

### **IV. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_.

## HIPAA Patient Request for Privacy Protections of PHI

---

### I. PURPOSE AND APPLICABILITY

HIPAA §164.522 grants a patient, or their designated representative, the right to request privacy protections for their PHI. Accordingly, the purpose of this Policy is to ensure that \_\_\_\_\_ has the proper procedure in place to handle such requests.

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.

### II. DETAILED POLICY STATEMENT

1. \_\_\_\_\_ must permit an individual to request that it restrict:

- Uses or disclosures about the individual to carry out treatment, payment, or health care operations; and
- Disclosures permitted under §164.510(b)

2. \_\_\_\_\_ is not required to agree to a request for restriction unless:

An individual requests to restrict the disclosure of PHI about the individual to a health plan and the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and the PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual has paid \_\_\_\_\_ in full.

3. If \_\_\_\_\_ agrees to a restriction then it may not use or disclose PHI in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment, then \_\_\_\_\_ may use the restricted PHI, or may disclose such information to a health care provider, to provide such treatment to the individual. Further, when restricted PHI is disclosed to a health care provider for emergency treatment, the covered entity must request that such health care provider not further use or disclose the information.

4. \_\_\_\_\_ and all Workforce Members must be aware that a restriction under §164.522(a) is not effective to prevent uses or disclosures that are permitted or required under §164.502(a)(2)(ii), §164.510(a), or §164.512.

5. \_\_\_\_\_ may terminate a restriction if:

- The individual agrees to or requests the termination in writing;
- The individual orally agrees to the termination and the oral agreement is documented; or
- The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is: Not effective for protected health information restricted under §164.522(a)(1)(vi); and only effective with respect to PHI created or received after it has so informed the individual.

6. Decisions pertaining to whether or not \_\_\_\_\_ will grant a request to restrict access to PHI must be made by the PO or his/her designee. All other Workforce Members must escalate such requests to the PO or his/her designee.
7. Confidential Communication Requirements. \_\_\_\_\_ must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of PHI from \_\_\_\_\_ by alternative means or alternative locations.
8. \_\_\_\_\_ may require the individual to make a request for a confidential communication in writing.
9. \_\_\_\_\_ may condition the provision of a reasonable accommodation on:
  - When appropriate, information as to how payment, if any, will be handled; and
  - Specification of an alternative address or other method of contact.
10. \_\_\_\_\_ may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

### **III. RESPONSIBILITY**

1. This Policy applies to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.
2. This Policy is to be implemented and maintained by the Privacy Officer.

### **IV. DOCUMENTATION**

All requests for restrictions on PHI and any correspondence related thereto, must be documented in writing and retained for 6 years from the date that such documents were created or the date when they were last in effect, whichever is later.

### **V. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_.

## HIPAA Patient Request to Access PHI

---

### I. PURPOSE AND APPLICABILITY

HIPAA §164.524 grants a patient, or their designated representative, the right to request access to their PHI in a designated record set. Accordingly, the purpose of this Policy is to ensure that \_\_\_\_\_ has the proper procedure in place to handle such requests.

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.

### II. DETAILED POLICY STATEMENT

1. \_\_\_\_\_ must permit an individual to request access to inspect or obtain a copy of their PHI that is maintained in a designated record set. The individual also has the right to direct \_\_\_\_\_ to transmit a copy of said information to a designated person or entity of the individual's choice. Individuals have a right to access this PHI for as long as the information is maintained by a covered entity, or by a business associate on behalf of a covered entity, regardless of the date the information was created; whether the information is maintained in paper or electronic systems onsite, remotely, or is archived; or where the PHI originated (e.g., whether the covered entity, another provider, the patient, etc.).
2. \_\_\_\_\_ must require individuals to make a request to access PHI in writing, and the \_\_\_\_\_ must provide the individual with advance notice of said requirement.
3. Whenever a request for access is properly made, the Workforce Member who receives the request shall forward the request to PHAMRACY'S CO. The CO or their designee are the only Workforce Members authorized to determine whether or not to comply with the request.
4. Whenever \_\_\_\_\_ receives such a request, it must act on the request within 30 days after receipt of the request. If \_\_\_\_\_ is unable to act on the request within the 30-day period, then it may extend the time needed to take appropriate action by no more than an additional 30 days, provided that:
  - \_\_\_\_\_ provides the individual with a written statement of the reasons for the delay and the date by which the \_\_\_\_\_ will complete its action on the request; and
  - \_\_\_\_\_ shall have only one such extension of time for action on a request for access
5. Unless an applicable exception applies, \_\_\_\_\_ must grant an individual's request to access their PHI.
6. If \_\_\_\_\_ denies access, in whole or in part, to PHI, then it must comply with the following requirements:

- \_\_\_\_\_ must, to the extent possible, give the individual access to any other PHI requested, after excluding PHI as to which \_\_\_\_\_ has grounds to deny access;
  - \_\_\_\_\_ must provide the individual with timely, written notice of the denial. The denial must be written in plain language and it must include: (1) the basis for the denial, (2) if applicable, a statement of the individual's review rights under §164.524(a)(4), including a description of how the individual may exercise such review rights, and (3) a description of how the individual may complain to \_\_\_\_\_ pursuant to §164.530(d) or to the Secretary of HHS pursuant to §164.306. The description must also include the name, or title, and number of the contact person or office designated in §164.530(a)(1)(ii).
7. If the individual has requested a review of a denial under §164.524(a)(4) of this section, \_\_\_\_\_ must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. \_\_\_\_\_ must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in §164.524(a)(3) of this section. \_\_\_\_\_ must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.
8. If \_\_\_\_\_ does not maintain the PHI that is the subject of the individual's request, and \_\_\_\_\_ knows where the requested information is maintained, then it must notify the individual where to direct the request for access.
9. \_\_\_\_\_ must provide the individual with access to PHI in the form and format requested by the individual, if it is readily producible in such format; or, if not, in a readable hard copy form or such other form and format as agreed to by \_\_\_\_\_ and the individual.
10. \_\_\_\_\_ must provide the access as requested by the individual in a timely manner as required by 164.524(b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or mailing the copy of the PHI at the individual's request. \_\_\_\_\_ may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.
11. Where applicable, \_\_\_\_\_ may provide an individual with a summary of PHI, in lieu of providing access to the PHI or may provide an explanation of the PHI to which access has been provided, if:
- The individual agrees in advance to such a summary or explanation; and
  - The individual agrees in advance to the fees imposed, if any, by \_\_\_\_\_ for providing such a summary or explanation.
12. If the individual requests a copy of the PHI or agrees to a summary or explanation of such information, \_\_\_\_\_ may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:
- i. Labor for copying the PHI requested by the individual, whether in paper or electronic form;



- ii. Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;
- iii. Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
- iv. Preparing an explanation or summary of the PHI, if agreed to by the individual as required by §164.524(c)(2)(iii).

### **III. RESPONSIBILITY**

1. This Policy applies to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.
2. This Policy is to be implemented and maintained by the Privacy Officer.

### **IV. DOCUMENTATION**

\_\_\_\_\_ must document the following:

1. The designated record sets that are subject to access by individuals; and
2. The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

\_\_\_\_\_ must maintain copies of the required documentation for a period of six (6) years from the date that such documents were created or the date when they were last in effect, whichever is later.

### **V. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_.

## HIPAA Patient Request to Amend PHI

---

### I. PURPOSE AND APPLICABILITY

HIPAA §164.526 grants an individual, or their designated representative, the right to have \_\_\_\_\_ amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set. Accordingly, the purpose of this Policy is to ensure that \_\_\_\_\_ has the proper procedure in place to handle such requests.

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.

### II. DETAILED POLICY STATEMENT

1. An individual has the right to have \_\_\_\_\_ amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.
2. \_\_\_\_\_ has the right to deny an individual's request for amendment, if it determines that the PHI or record is that is the subject of the request:
  - Was not created by \_\_\_\_\_, unless the individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested information;
  - Is not part of the designated record set;
  - Would not be available for inspection under §164.524; or
  - Is accurate and complete.
3. \_\_\_\_\_ must require that an individual submit a request to amend PHI in writing. The writing must provide a reason as to why the PHI should be amended. \_\_\_\_\_ must provide advance notice to patients of its process for receiving requests to amend PHI. Namely, it must make clear that all requests must be in writing and specify the reason as to why an amendment is appropriate.
4. \_\_\_\_\_ must take timely action when responding to requests to amend PHI. Accordingly, \_\_\_\_\_ must act on an individual's request to amend PHI no later than 60 days after receipt of said request. If \_\_\_\_\_ is unable to take action within this timeframe then \_\_\_\_\_ then it may extend the time for such action by no more than 30 days, provided that:
  - \_\_\_\_\_, within the initial 60 day window to act, notifies the individual through a written statement with the reasons for the delay and the date by which \_\_\_\_\_ will complete its action on the request; and
  - \_\_\_\_\_ may only have one such extension of time for such action on a request for an amendment.

5. Where \_\_\_\_\_ accepts a request to amend PHI, it must comply with the following:
- It must timely -within 60 days from receipt of the request – make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the amendment;
  - It must timely notify the individual that the amendment has been accepted and obtain the individual's consent to have \_\_\_\_\_ notify relevant persons with which the amendment needs to be shared; and
  - It must make reasonable efforts to inform and provide the amendment within a reasonable time to: (1) persons identified by the individual as having received PHI about the individual and needing the amendment, and (2) to persons, including business associates, that \_\_\_\_\_ knows have the PHI that is the subject of the amendment and that they may have relied, or could foreseeably rely, on such information to the detriment of the individual.
6. If \_\_\_\_\_ denies a request to amend PHI then it must comply with the following:
- It must provide the individual with a timely, written denial. The denial must use plain language and contain:
  - The basis for the denial
  - The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
  - A statement that, if the individual does not submit a statement of disagreement, the individual may request \_\_\_\_\_ to provide the individual's request for amendment and the denial with any future disclosures of PHI that is the subject of the amendment; and
  - A description of how the individual may complain to \_\_\_\_\_ pursuant to the complaint procedures established in §164.530(d) or to the Secretary of HHS pursuant to the procedures established in §164.306. The description must include the name, or title, and phone number of the contact person or office designated in §164.530(a)(1)(ii).
7. When \_\_\_\_\_ issues a denial, it must allow the individual to submit a written statement of disagreement. \_\_\_\_\_ may reasonably limit the length of the statement.
8. At its discretion, \_\_\_\_\_ may issue a rebuttal statement to the individual's statement of disagreement. Whenever this is done, \_\_\_\_\_ must provide a copy of the rebuttal statement to the individual who submitted the statement of disagreement.

9. When making future disclosures of PHI, \_\_\_\_\_ must review and ensure compliance with the requirements set forth under §164.526(5).
10. The PO or his/her designee must make all determinations as to whether or not to accept a request to amend PHI or a record. All other Workforce Members who receive such a request must escalate it to the PO or their designee.

### **III. RESPONSIBILITY**

1. This Policy applies to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.
2. This Policy is to be implemented and maintained by the Privacy Officer.

### **IV. DOCUMENTATION**

\_\_\_\_\_ must document the following:

1. \_\_\_\_\_ must, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, \_\_\_\_\_'S denial of the request, the individual's statement of disagreement, if any, and the PHARAMCY'S rebuttal, if any, to the designated record set.

In addition, \_\_\_\_\_ must document any actions taken in regards to the request, any rebuttals, statements of disagreement, etc. \_\_\_\_\_ must also document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by §164.530(j).

Any documentation required under this Policy must be retained for 6 years from the date that such documents were created or the date when they were last in effect, whichever is later.

### **V. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_.

## HIPAA Patient Request to Receive Accounting of PHI

---

### I. PURPOSE AND APPLICABILITY

HIPAA §164.528 grants an individual, or their designated representative, the right to receive an accounting or disclosures of PHI. Accordingly, the purpose of this Policy is to ensure that \_\_\_\_\_ has the proper procedure in place to handle such requests. This Policy is applicable to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.

### II. DETAILED POLICY STATEMENT

1. An individual has a right to receive an accounting of disclosures of protected health information made by \_\_\_\_\_ in the six years prior to the date on which the accounting is requested, except for disclosures:
  - To carry out treatment, payment and health care operations as provided in § 164.506;
  - To individuals for whom PHI was created or obtained as provided in § 164.502;
  - Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502;
  - Pursuant to an authorization as provided in § 164.508;
  - For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510;
  - For national security or intelligence purposes as provided in § 164.512(k)(2);
  - To correctional institutions or law enforcement officials as provided in § 164.512(k)(5);
  - As part of a limited data set in accordance with § 164.514(e); or
  - That occurred prior to the compliance date for the covered entity.
2. Whenever a request for an accounting of PHI is received by a Workforce Member, said member must forward the request to \_\_\_\_\_'S PO or the PO's designee. Only the PO and their designee are authorized to act on such requests.
3. \_\_\_\_\_ must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.
4. If an agency or official makes such a statement orally, as opposed to in writing, then \_\_\_\_\_ must:

- Document the statement, including the identity of the agency or official making the statement;
  - Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and
  - Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to §164.528(a)(2)(i) is submitted during that time.
5. \_\_\_\_\_ must allow an individual to request an accounting for disclosures for a period of time that is less than 6 years from the date of the request.
6. Regarding the content of the accounting, \_\_\_\_\_ must provide the individual with a written accounting that:
- Except as otherwise provided in §164.528(a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in §164.528 (a)(3)) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.
  - Except as otherwise provided in §164.528 (b)(3) or (b)(4), the accounting must include for each disclosure:
    - The date of the disclosure;
    - The name of the entity or person who received the protected health information and, if known, the address of such entity or person;
    - A brief description of the protected health information disclosed; and
    - A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under § 164.502(a)(2)(ii) or § 164.512, if any.
7. If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under § 164.502(a)(2)(ii) or § 164.512, the accounting may, with respect to such multiple disclosures, provide:
- The information required by §164.528(b)(2) for the first disclosure during the accounting period;
  - The frequency, periodicity, or number of the disclosures made during the accounting period; and
  - The date of the last such disclosure during the accounting period.
8. If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in accordance with § 164.512(i) for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:
- The name of the protocol or other research activity;

- A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;
  - A brief description of the type of protected health information that was disclosed;
  - The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
  - The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
  - A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.
9. \_\_\_\_\_ must act on an individual's request for an accounting, no later than 60 days after receipt of such request. \_\_\_\_\_ must provide the individual with the accounting requested, or if it is unable to do so within the 60-day period, then it may extend the time to comply by an additional 30 days, provided that:
- Within the initial 60 day period, \_\_\_\_\_ provides the individual with a written statement of the reasons for the delay and the date by which \_\_\_\_\_ will provide the accounting; and
  - \_\_\_\_\_ may have only one such extension of time for action on a request for an accounting.
10. \_\_\_\_\_ must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

### **III. RESPONSIBILITY**

1. This Policy applies to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.
2. This Policy is to be implemented and maintained by the Privacy Officer.

### **IV. DOCUMENTATION**

\_\_\_\_\_ must document the following:

1. The information required to be included in an accounting under §164.528(b) for disclosures of protected health information that are subject to an accounting under §164.528(a);
2. The written accounting that is provided to the individual under this section; and
3. The titles of the person(s) or offices responsible for receiving and processing requests for an accounting by individuals.

All such documentation must be retained for 6 years from the date that such documents were created or the date when they were last in effect, whichever is later.

**V. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_.



## HIPAA Minimum Necessary Policy

---

### I. PURPOSE AND APPLICABILITY

The Minimum Necessary Standard element of the Privacy Rule requires \_\_\_\_\_ to take reasonable steps to limit the release of PHI to the minimum necessary to accomplish the intended purpose behind the use, disclosure, or request. The purpose of this Policy is to ensure that \_\_\_\_\_ has the proper procedures in place to comply with the Minimum Necessary Standard per HIPAAA §164.514(d).

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.

### II. DETAILED POLICY STATEMENT

1. The Minimum Necessary Standard requires \_\_\_\_\_ to take reasonable steps to limit the release of PHI to the minimum necessary to accomplish the intended purpose behind the use, disclosure, or request.
2. The standard is designed to be flexible and thus allows \_\_\_\_\_ discretion to determine how best to implement appropriate procedures to comply with the rule. Accordingly, the Privacy Officer must evaluate the various ways in which \_\_\_\_\_ uses and discloses PHI and then implement procedures that comply with the Minimum Necessary Standard.
3. \_\_\_\_\_ must identify the persons or class of persons within its Workforce who require access to PHI in order to carry out their duties.
4. For each such person or class, \_\_\_\_\_ must determine the category/categories of PHI to which access is necessary and any conditions appropriate to such access.
5. \_\_\_\_\_ must take reasonable steps to limit access to only those persons/classes who have been determined to require access.
6. For disclosures that \_\_\_\_\_ makes on a routine and recurring basis, it must implement policies and procedures that limit PHI to only the amount necessary to achieve the purpose of the disclosure.
7. For all other disclosures, \_\_\_\_\_ must develop criteria designed to limit PHI disclosed to only the amount reasonably necessary to accomplish the purpose for which the disclosure is sought and review requests for disclosure on an individual basis in accordance with such criteria.
8. \_\_\_\_\_ may rely on the statement of others in determining the minimum necessary if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose:
  - when the requested is coming from a public officials, another covered entity, a professional who is a member of \_\_\_\_\_'S workforce, is a business

associate of the \_\_\_\_\_, or by a person requesting the information for research purposes that complies with § 164.512(i), and

- The public officials, covered entity, member of \_\_\_\_\_'S workforce, business associate of the \_\_\_\_\_, or person requesting the information for research purposes represents that the information requested is the minimum necessary for the stated purpose(s)

9. The Minimum Necessary Standard does not apply to:

- Disclosures to or requests by a health care provider for treatment;
- Uses or disclosures made to the individual, or as required when an individual asks for access or an accounting of their PHI record;
- Uses or disclosures made pursuant to an individual's authorization;
- Uses or disclosures that are required by law as explained under §164.512(a); and
- Any other uses or disclosures that are required for compliance under Subpart E of Part 164, i.e., the Privacy Rule Subpart.

### **III. RESPONSIBILITY**

1. This Policy applies to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.
2. This Policy is to be implemented and maintained by the Privacy Officer.

### **IV. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_.

## HIPAA PHI Use & Disclosure Policy

---

### I. PURPOSE AND APPLICABILITY

The Privacy Rule seeks to define and limit the extent to which an individual's PHI may be used/disclosed. \_\_\_\_\_, as a covered entity, may not use or disclose a patient's PHI unless: (1) the Privacy Rule permits or requires such action, or (2) as a patient – who is the subject of such PHI – or their personal representative authorizes in writing. The purpose of this Policy is to ensure that \_\_\_\_\_ understands when it is legally allowed to use/disclose PHI under HIPAA. While this Policy provides a thorough overview of the various types of disclosures that are permitted under HIPAA, it is not intended to be a definitive guide as to whether or not \_\_\_\_\_ is legally allowed to use or disclose PHI under HIPAA. Accordingly, to the extent that a Workforce Member has questions regarding the use or disclosure of PHI, said individual must consult with the Privacy Officer.

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.

Note: Where \_\_\_\_\_ is permitted under HIPAA to make a disclosure of PHI, the disclosure can be made orally, in writing, by phone, fax, or otherwise, provided that \_\_\_\_\_ has taken appropriate steps to reasonably safeguard the information from unpermitted access. Whether an action constitutes a reasonable safeguard is fact specific. For example, when faxing PHI to a telephone number that is not regularly used, a reasonable safeguard might involve a member of \_\_\_\_\_'S workforce calling ahead to confirm the accuracy of the fax number.

### II. DETAILED POLICY STATEMENT

#### Permitted Disclosures

1. The Privacy Rule seeks to define and limit the extent to which an individual's PHI may be used/disclosed. \_\_\_\_\_, as a covered entity, may not use or disclose a patient's PHI unless: (1) the Privacy Rule permits or requires such action, or (2) as a patient – who is the subject of such PHI – or their personal representative authorizes in writing. The Privacy Rule permits, but does not require \_\_\_\_\_ (as a covered entity) to voluntarily obtain patient consent for uses and disclosures of PHI for treatment, payment, and healthcare operations.

HIPAA defines treatment to include such things as: the provision, coordination, or management of health care and related services (including coordination and management by a provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one provider to another). In the \_\_\_\_\_ context this can include discussions regarding a patient with a provider to discuss potential adverse medication reactions, as well as a patient's medication and health history.

Payment includes, but is not limited to, activities pertaining to coverage and eligibility determinations, claims management, billings, collections, review of services relating

to medical necessity or justification for charges, utilization review activities, and certain disclosures (e.g., name, DOB, account number) to consumer reporting agencies.

Business operations include those activities which are necessary to conduct quality assessments and improvement activities, which include contacting patients and health care providers with information regarding treatment alternatives. Examples include: disclosing medical information to assess the use or efficacy of a particular drug, developing and monitoring medical protocols, and to provide medication reminders within the parameters of the Privacy Rule.

## 2. Family Members and Caregivers

Disclosing to a family member, other relative, close personal friend, or any other person identified by the individual, the PHI directly related to such person's involvement with the individual's health care or payment related to the individual's health care. \_\_\_\_\_ may also use and/or disclose PHI to notify, or assist in the notification of a family member, a caregiver, or the designated representative of the patient, regarding the patient's location, general condition, or death.

If the individual is present or otherwise available prior to the use or disclosure, and has the mental capacity necessary to make health care related decisions, then the information may be disclosed only if: the individual consents, is provided with an opportunity to object, or the treating pharmacist can reasonably infer from the individual's conduct – based on the exercise of professional judgement – that the individual does not object to the disclosure;

Where an individual is not present, or cannot object due to incapacity, or is emergency circumstance, then the pharmacist may disclose the PHI – if in exercising professional judgement – he/she determines that it is in the patient's best interest and the information to be disclosed is directly relevant to the person's involvement with the individual's care or payment related to the individual's care, or needed for notification purposes. Where an individual is deceased, \_\_\_\_\_ may disclose PHI of the individual to a person who was involved in the individual's care or payment of health care prior to the individual's death, unless doing so is inconsistent with any prior expressed preference of the of the individual that is known to \_\_\_\_\_.

## 3. Limited Data Sets

\_\_\_\_\_ may use or disclose a patient's PHI in accordance with the Privacy Rule's requirements regarding limited data sets and;

## 4. Disaster Relief Purposes

\_\_\_\_\_ may use or disclose PHI to a public or private entity authorized by law or its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by §164.510(b)(1)(ii) which is cited in the preceding bullet point and which pertains to notifying appropriate persons of an individual's location, general condition, or death. Any such use or disclosure must comply with the above-mentioned objection requirements regarding instances where the individual is present, not present, or deceased, as the case may be.

## 5. Victims of Abuse, Neglect, or Domestic Violence

If \_\_\_\_\_ reasonably suspects that a child is the victim of abuse or neglect then it may use or disclose PHI to appropriate governmental authorities and/or others authorized by law to receive reports of child abuse/neglect.

If \_\_\_\_\_ reasonably suspects that an adult is the victim of abuse or neglect, then it may use or disclose PHI, as required by law, to a government authority – including a social service or protective services agency - authorized by law to receive such reports and information so long as \_\_\_\_\_, in the exercise of its professional judgement, believes that the disclosure is necessary to prevent serious harm to the individual or other potential victims; or a law enforcement or other public official authorized to receive the report represents that the PHI is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

If \_\_\_\_\_ makes a disclosure permitted by this paragraph then it must promptly inform the individual that such a report has been or will be made, except if:

- The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
- The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

## 6. Public Health Activities

\_\_\_\_\_ may release PHI to a public health authority to: (1) respond to natural or man-made disasters in which the release of PHI is necessary to effectuate proper treatment for affected individuals, (2) curb serious threats to health and safety, (2) prevent or lessen an imminent threat to the health or safety of a person or the public, provided that such release is made to a person/agency who is potentially able to eradicate the threat, (3) prevent or control disease, injury, or disability, (4) or to report adverse reactions to medications, deficiencies in products, recalls, and situations in which a patient needs to be notified of potential exposure to a communicable disease.

## 7. Judicial or Administrative Proceedings

In accord with any applicable Federal and State laws, \_\_\_\_\_ may disclose PHI in a judicial or administrative proceeding in response to: a court order, subpoena, discovery request, or other lawful process in accord with the following:

\_\_\_\_\_, in response to a court order, may disclose PHI in a judicial or administrative proceeding expressly authorized by such order.

\_\_\_\_\_, in response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

- \_\_\_\_\_, receives satisfactory assurance as defined by § 164.512 (e)(1) (iii) –(iv) from the party seeking the information that either a reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or that reasonable efforts have been made by such party to secure a qualified protective order as defined in § 164.512 (e)(1)(v); or
- \_\_\_\_\_ makes reasonable efforts to provide the individual sufficient to meet the requirements of §164.512 (e)(1) (iii) or seeks a qualified protective order sufficient to meet the requirements of § 164.512 (e)(1)(v).

#### 8. Health and Safety

\_\_\_\_\_ may disclose PHI to prevent a serious threat to health and safety provided it believes in good faith that the information is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and the report is supplied to a person or persons who are reasonably able to prevent or lessen the threat, including the target of threat.

#### 9. Specialized Government Functions

\_\_\_\_\_ may use or disclose PHI for other specialized government functions, including authorized Federal officials for the conduct of lawful intelligence, counterintelligence, and other national security activities that are authorized under Federal law. \_\_\_\_\_ may also disclose PHI for medical suitability determinations requested by the US Department of State.

#### 10. Worker's Compensation

\_\_\_\_\_ may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

### Required Authorizations

1. HIPAA Section 164.508 makes clear that patient authorization is required prior to using/disclosing the PHI under the following circumstances: (1) if the use or disclosure is not otherwise permitted by HIPAA, (2) if the use/disclosure is for marketing purposes except when communication occurs face to face between \_\_\_\_\_ and the patient or when the communication involves a promotional gift on nominal value, (3) if the use/disclosure involves psychotherapy notes other than for specific treatment, payment, or healthcare operations (see HIPAA Section 164.508(a)(2)(i) and (a)(2)(ii)), (4) if the use/disclosure is for research purposes, or (5) if the use/disclosure involves the sale of PHI. Where the Privacy Rule requires authorization, voluntary patient consent is insufficient to permit a use/disclosure of PHI unless it meets the requirements of a valid authorization.

In addition to the above, other Federal and many state laws also provide privacy protections for certain classes of PHI above and beyond the protections generally

provided by HIPAA. The following classes of information are among those requiring special consideration:

- i. Substance abuse records,
- ii. Psychotherapy notes,
- iii. Aids test results,
- iv. Genetic information,
- v. Mental health records,
- vi. Mental retardation records,
- vii. Mental health research results, and
- viii. Controlled substance research results.

The core elements of a valid authorization include:

- A meaningful description of the information to be disclosed.
  - The name – or other specific identification - of the individual or class of persons authorized to make the requested use or disclosure.
  - The name - or other specific identification - of the individual or class of persons to whom \_\_\_\_\_ may make the requested use or disclosure.
  - A description of each purpose of the disclosure. The statement, “At the request of the individual,” is sufficient when the individual initiates the authorization and does not, or elects not to, provide a statement of the purpose. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.
  - A signature of the individual or their personal representative (someone authorized to make healthcare decisions on behalf of the individual; see Section 6 of this Policy) and the date.
  - If the authorization pertains to marketing involving a financial remuneration -as defined in paragraph (3) of the definition of marketing at § 164.501 - to the covered entity from a third party, then authorization must state that such remuneration is involved.
  - Also, notwithstanding any provision of subpart E of Part 164, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart. (ii) Such authorization must state that the disclosure will result in remuneration to the covered entity
2. In addition to the core elements, the authorization must comply with the “required statements” addressed in §164.508(c)(2)-(c)(4). \_\_\_\_\_ should consult the cited code section to ensure compliance, but generally speaking, the cited section requires \_\_\_\_\_ to:
- Make the individual aware of his/her right to revoke the authorization in writing;
  - Explain the exceptions to the right to revoke and provide a description of how the individual may revoke the authorization;

- The ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization; and
  - Explain that the potential for information disclosed through an authorization may be subject to redisclosure by the recipient and consequently, no longer protected under the Privacy Rule.
3. The authorization is required to be written in “plain language” so that it is easily understood by all.
  4. Where \_\_\_\_\_ seeks an authorization from an individual for a use/disclosure of PHI, it must provide the individual with a copy of the signed authorization (assuming that the individual in question complies with the request).
  5. \_\_\_\_\_ is required to retain documentation of any signed authorizations. The documentation must be recorded in written form (which may be electronic) and it must be retained for 6 years from the date of its creation or the date when it last was in effect, whichever is longer.

### **Mandatory Disclosures**

1. The Privacy Rule requires \_\_\_\_\_ to make a mandatory disclosure under two circumstances. First, to individuals/ their representatives when they request access to, or any accounting of their PHI. Second, when required by the Secretary of the US Department of Health and Human Services (HHS) for the purpose of a review, investigation, or enforcement action. Where disclosure of PHI is required due to investigatory matters, or is otherwise permitted under the Privacy Rule, such required disclosures take precedent over the privacy rights of the patient under HIPAA. Notwithstanding this fact, HIPAA does not deny a workforce member the ability to request and verify certain information from the requesting party. If a workforce member is ever asked to comply with a mandatory disclosure request, the workforce member must immediately notify their supervisor or Compliance Officer, and comply with the following procedure:
2. The workforce member must notify the requestor that the workforce employee must report the request to \_\_\_\_\_’S Compliance Officer and comply with an internal process prior to releasing the requested information.
3. If the request is made in person, then the workforce employee must immediately notify the Compliance Officer.
4. If the Compliance Officer is unavailable then the workforce member must inform their supervisor or \_\_\_\_\_ manager. The supervisor or manager must take control of the situation.
5. The supervisor or manager must then make an effort to reach the Compliance Officer. If the Compliance Officer remains unavailable then the supervisor or manager may, at their discretion, comply with the request provided that the supervisor or manager has been trained on the specifics of this Policy and collects all pertinent identification from the requestor as well as a signed release form.



6. If the requestor appears in person then make sure that said person meets the definition of an "Official" as defined under this Policy.
7. Use the Mandatory Disclosure Form affixed to the end of this to gather all pertinent information and to verify the identity of the requestor.
8. Always ask for a copy of the request and of the I.D. of the requestor. Affix a copy of the I.D. to the copy of the request and sign and date it.
9. If the disclosure request does not include an actual written document then the requestor must fill out the section on the form that pertains to the reason for the request, the name of the patient whose records are being requested, and any other relevant information.
10. In keeping with the minimum necessary standard, the information released should be only the amount necessary to comply with the purpose of the request. Accordingly, the information released should be specific in nature. Such information might include prescription information, or identification information.
11. If a law enforcement official or other government agent asks to speak with the patient then the Compliance Officer – or the supervisor/manager in the event that the Compliance Officer is unavailable – may comply with the request only if he/she is of the opinion that such compliance would not hinder the patient's care.
12. Where the Compliance Officer or supervisor/manager agrees to the request, the patient must be asked whether he/she is willing to speak with government official. The patient is under no obligation to speak to the official, and thus, if he/she does not wish to speak with the official, then \_\_\_\_\_ will abide by the wishes of the patient. This rule is to apply even in instances where the patient is an alleged perpetrator of a crime.
13. Under no circumstances shall mental health, HIV/AIDS, or genetic information be disclosed without the written consent of the patient or his/her legal representative.

#### 14. Administrative & Judicial Requests

The Compliance Officer or supervisor/manager may disclose PHI in the course of any administrative or judicial proceeding, any court order or administrative tribunal (to the extent that such a disclosure is authorized) or in response to a subpoena or discovery request. These types of requests must be submitted to the Privacy Officer, who must then discuss the matter with \_\_\_\_\_'S legal counsel prior to fulfilling the request.

#### 15. Law Enforcement Requests

If the requestor of PHI is a member of law enforcement, then the Compliance Officer or supervisor/manager may release PHI under the following circumstances: (1) to identify or locate a suspect, fugitive, material witness, or missing person; (2) to identify the victim of a crime, including instances where \_\_\_\_\_ is unable to obtain the victims' authorization; (3) to identify facts or persons pertaining to a death

that is being investigated as the result of criminal conduct; or (4) in response to a court order, subpoena, warrant, summons, or similar process.

16. Requests from the Military & Homeland Security

Compliance Officer or supervisor/manager may release PHI if requested to do so by military or national security agencies. All such requests must be dealt with by the Compliance Officer. Appropriate requests will usually pertain to matters of local/national security, intelligence purposes in conformity with the National Security Act, and for protective services of the President and other government personnel. If confronted with such a scenario, the Compliance Officer is highly encouraged to consult \_\_\_\_\_'S attorney prior to complying with such a request.

**III. RESPONSIBILITY**

1. All Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. This Policy is to be implemented and maintained by the Privacy Officer.

**IV. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_..

## **HIPAA Personal Representative Policy**

### **I. PURPOSE AND APPLICABILITY**

HIPAA §164.502(g)(1) requires that covered entities treat personal representatives as the individual for purposes of the Privacy Rule. Under the Rule, an individual's personal representative is someone authorized under State or other applicable law to act on behalf of the individual in making health care related decisions. With respect to deceased individuals, the individual's personal representative is an executor, administrator, or other person who has authority under State or other law to act on behalf of the deceased individual or the individual's estate. Thus, whether a family member or other person is a personal representative of the individual, and therefore has a right to access the individual's PHI under the Privacy Rule, generally depends on whether that person has authority under State law to act on behalf of the individual. See 45 CFR 164.502(g) and 45 CFR 164.524. Accordingly, this Policy is designed to ensure that \_\_\_\_\_ has the proper procedures in place to handle access requests to PHI that are made by personal representatives.

Outside of the HIPAA right of access, other provisions in the Privacy Rule address disclosures to family members. Specifically, a covered entity is permitted to share information with a family member or other person involved in an individual's care or payment for care as long as the individual does not object. In cases where the individual is incapacitated, a covered entity may share the individual's information with the family member or other person if the covered entity determines, based on professional judgment, that the disclosure is in the best interest of the individual. If the individual is deceased, a covered entity may make the disclosure unless doing so is inconsistent with any prior expressed preference of the individual. These disclosures are generally limited to the health information that is relevant to the person's involvement in the individual's care or payment for care. See 45 CFR 164.510(b).

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_.

### **II. REQUIREMENTS**

1. \_\_\_\_\_ acknowledges an individual's right to appoint a personal representative to inspect and receive a copy of the individual's PHI.
2. Before PHI may be disclosed to a personal representative, the Privacy Officer or his/her designee must verify the person's authority to act as a personal representative under applicable law, by obtaining one of the following document types: a court order, guardianship, a notarized and authenticated statement granting such rights, or through executing \_\_\_\_\_'S personal designation form which must then be accepted by the Privacy Officer.
3. Only the Privacy Officer or his/her designee may determine whether a person has submitted sufficient documentation to sufficiently prove their status as a personal

representative, and thus be entitled to inspect and receive a copy of an individual's PHI.

4. Once a person's status as a personal representative has been verified, the person shall have the authority to act on behalf of the individual in regards to PHI. This means that the personal representative will have the authority to request access, accounting, and/or restrictions on the manner in which \_\_\_\_\_ uses or discloses the individual's PHI.
5. When a request for access, disclosure, or restriction of the ways in which \_\_\_\_\_ uses and discloses an individual's PHI is made by a personal representative, then all Workforce Members must follow the appropriate procedure, as described, in the HIPAA PHI Use & Disclosure Policy.
6. Despite the general rule that \_\_\_\_\_ must treat a personal representative who has the authority to make health care decisions on behalf of the individual, as the individual for the purposes of accessing, disclosing, or restricting PHI, several exceptions apply. Namely, exceptions exist where an unemancipated minor may lawfully obtain health care service without the consent of a parent, guardian, etc., in instances in which a court, or another person authorized by law consents to such health care service. Further, if a parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between the health care provider and the minor with respect to the rendering of a health care service, then said parent, guardian, etc., will not be permitted under HIPAA to act as a personal representative for the purposes of accessing PHI. Additionally, notwithstanding any applicable state laws, \_\_\_\_\_ may elect not to treat a person as the personal representative of an individual if \_\_\_\_\_ has a reasonable belief that the individual has been or will be subjected to domestic violence by the personal representative, or that treating such person as the personal representative could endanger the individual and \_\_\_\_\_ believes through exercising professional judgment that recognizing the person as a personal representative is not in the best interest of the individual. The above is not intended to be an exhaustive list of exceptions. Please consult §164.502 for additional information.
7. Notwithstanding anything to the contrary, \_\_\_\_\_ may allow any person – whether or not he/she is a personal representative – to pick up a filled prescription for an individual if through professional judgement and its experience with common practice, \_\_\_\_\_ determines that it's in the individual's best interest to allow said person to so act.

### **III. RESPONSIBILITY**

1. All Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. This Policy is to be implemented and maintained by the Privacy Officer.

### **IV. DOCUMENTATION**

\_\_\_\_\_ must maintain documentation that all required breach notifications were made, or alternatively documentation to demonstrate that notification was not required because (1) it conducted a risk assessment and found a low probability that PHI had been compromised by an impermissible use or disclosure; or (2) any other applicable exception to the definition of “breach” was applicable. \_\_\_\_\_ must maintain copies of the required documentation for a period of six (6) years from the date that such documents were created.

## **V. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_.

## **Business Associate Policy**

### **I. PURPOSE AND APPLICABILITY**

The following policy is designed to ensure that \_\_\_\_\_ and all of its workforce members are handling PHI appropriately when interacting with Business Associates (BAs).

This Policy is applicable to all Workforce Members

### **II. REQUIREMENTS**

1. A Business Associate (BA) is a person or entity that performs certain functions or services that involve the use or disclosure of PHI on behalf of, or for the benefit of, \_\_\_\_\_. \_\_\_\_\_'S own workforce members are not BAs. \_\_\_\_\_ itself, under certain circumstances, can be a BA. Specifically, the Privacy Rule asserts that providing activities or services such as payment or health care operation activities, among others, can make \_\_\_\_\_ a BA, provided the activity or service involves the use or disclosure of PHI. Below is a non-exhaustive list of the types of activities and services that may make a person or entity a BA as defined under HIPAA §160.103.

- BA functions and activities include: billing, benefit management, claims processing, data analysis, quality assurance, and utilization review.
- BA services include: accounting, accreditation, actuarial, consulting, data aggregation, financial, and legal.
- Under the Privacy Rule, PHARAMCY may disclose PHI to BAs and may allow BAs to create, receive, maintain, or transmit PHI on its behalf. In order to do so, \_\_\_\_\_ must obtain satisfactory assurance that the BA will appropriately safeguard the information. In order for an assurance to be satisfactory, HIPAA requires that the assurance be evidenced by a written agreement or arrangement that meets the requirements set forth at §164.504(e). Namely, the contract must:
  - i. Establish the permitted and required uses and disclosures of PHI by the BA;
  - ii. Establish that the BA must not use or further disclose PHI other than as permitted or required by the contract or law; \
  - iii. Require that the BA uses appropriate safeguards and comply, where applicable, with subpart C of Part 164 with respect to ePHI, to prevent use or disclosure of the information other than as provided for by its contract;
  - iv. Require that the BA report to \_\_\_\_\_ any instances in which information was used or disclosed in a manner not provided for under the contract of which it becomes aware, including breaches of unsecured PHI;
  - v. \_\_\_\_\_'s contract with a BA must always include language which ensures that any subcontractor that creates, receives, maintains, or transmits

PHI on behalf of a BA is bound by the same restrictions and conditions regarding PHI, that the BA is bound by;

- vi. Make available PHI in accordance with §164.524;
  - vii. Make available PHI for amendment and incorporate any amendments to PHI in accordance with §164.526;
  - viii. Make available the information required to provide an accounting of disclosures in accordance with §164.528;
  - ix. If a BA is to carry out any of the obligations of \_\_\_\_\_ under this subpart (i.e. subpart E of Part 164) comply with the requirements of this subpart that apply to \_\_\_\_\_ in the performance of such obligation;
  - x. The BA must make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the BA on behalf of, the covered entity available to the Secretary of HHS for purposes of determining the covered entities compliance with Subpart E of Part 164 of the Act;
  - xi. At termination of the contract, if feasible, BA must return or destroy all PHI received from, or created or received by the BA on behalf of, the covered entity that the BA still maintains in any form and retain no copies of such information and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible; and
  - xii. BA must agree to authorize termination of the contract by the covered entity, if the covered entity determines that the BA has violated a material term of the contract.
2. \_\_\_\_\_ is not in compliance with §164.502(e) and §164.504(e) – the requirements of which were discussed in the preceding paragraph – if \_\_\_\_\_ knew of a pattern or activity or practice of the BA that constituted a material breach or violation of the BA's obligation under the contract or other arrangement, unless \_\_\_\_\_ took reasonable steps to cure the breach or end the violation, as applicable., and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible. In the event that termination of the contract is not feasible, then \_\_\_\_\_ must report the issue to HHS' Office for Civil Rights. Further, in instances in which \_\_\_\_\_ is a BA and engaging with a subcontractor then \_\_\_\_\_ must comply with §164.504 (e)(1) (iii). In pertinent part, said section states that a business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.
3. It is \_\_\_\_\_'S policy that the Compliance Officer must determine if a contracted business activity requires a BA Agreement. If the Compliance Officer is unable to determine if a BA Agreement is required then he/she must consult with \_\_\_\_\_'S attorney.

4. Where an individual or entity is determined to be a BA of \_\_\_\_\_ it must sign a BA Agreement. A sample BA Agreement is included in this Policy for your convenience.
5. Either party may supply the BA Agreement. Where the BA provides the BA Agreement, such agreement must contain all of the elements listed under section d of this Business Associate Policy.
6. A BA Agreement will be executed only by those workforce members who have actual authority to enter into contractual agreements on behalf of \_\_\_\_\_.  
Notwithstanding the above, in all circumstances, the workforce member is to consult with, and must gain approval from the Compliance Officer, prior to executing any BA Agreement.
7. If issues or disputes pertaining to the executed BA Agreement arise, then \_\_\_\_\_'S Compliance Officer must be notified in a timely manner.
8. Minimum Necessary Disclosures. \_\_\_\_\_ staff must ensure that all disclosures to Business Associates are limited to the minimum amount of information needed for the Business Associate to carry out its functions on behalf of \_\_\_\_\_, unless an exception to the minimum necessary rule applies by law or pursuant to \_\_\_\_\_'s policies.
9. Any workforce member who does not abide by this Business Associate Policy is subject to disciplinary action, up to and including termination of employment.
10. Any BAs who are found to be in violation of any applicable policies or laws pertaining to fulfilling their obligations under the BA Agreement are subject to termination of the Agreement, and may be reported to the appropriate government agency if their actions are found to be in violation of HIPAA.

### **III. RESPONSIBILITY**

1. All Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. This Policy is to be implemented and maintained by the Privacy Officer.

### **IV. DOCUMENTATION**

\_\_\_\_\_ must retain Business Associate agreements for a period of six (6) years from the date that such documents were created.

### **V. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_.



## **Sample Business Associate Agreement Provisions**

Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions.

### **Definitions**

#### **Catch-all definition:**

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

#### **Specific definitions:**

(a) **Business Associate.** “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) **Covered Entity.** “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

(c) **HIPAA Rules.** “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

### **Obligations and Activities of Business Associate**

Business Associate agrees to:

- (a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;
- (b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;
- (c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

[The parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

- (d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on

behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available protected health information in a designated record set to the [Choose either “covered entity” or “individual or the individual’s designee”] as necessary to satisfy covered entity’s obligations under 45 CFR 164.524;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide the requested access or whether the business associate will forward the individual’s request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity’s obligations under 45 CFR 164.526;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual’s request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]

(g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either “covered entity” or “individual”] as necessary to satisfy covered entity’s obligations under 45 CFR 164.528;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business associate will forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity.]

(h) To the extent the business associate is to carry out one or more of covered entity’s obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

### **Permitted Uses and Disclosures by Business Associate**

(a) Business associate may only use or disclose protected health information

[Option 1 – Provide a specific list of permissible purposes.]

[Option 2 – Reference an underlying service agreement, such as “as necessary to perform the services set forth in Service Agreement.”]

[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the business associate will de-identify the information and the permitted uses and disclosures by the business associate of the de-identified information.]

(b) Business associate may use or disclose protected health information as required by law.

(c) Business associate agrees to make uses and disclosures and requests for protected health information

[Option 1] consistent with covered entity's minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity's minimum necessary policies and procedures.]

(d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add “, except for the specific uses and disclosures set forth below.”]

(e) [Optional] Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

(f) [Optional] Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) [Optional] Business associate may provide data aggregation services relating to the health care operations of the covered entity.

### **Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions**

(a) [Optional] Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's use or disclosure of protected health information.

(b) [Optional] Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.

(c) [Optional] Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's use or disclosure of protected health information.

### **Permissible Requests by Covered Entity**

[Optional] Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity. [Include an exception if the business associate will use or disclose protected health information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

### **Term and Termination**

(a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement [and business associate has not cured the breach or ended the violation within the time specified by covered entity]. [Bracketed language may be added if the covered entity wishes to provide the business associate with an opportunity to cure a violation or breach of the contract before termination for cause.]

(c) Obligations of Business Associate Upon Termination.

[Option 1 – if the business associate is to return or destroy all protected health information upon termination of the agreement]

Upon termination of this Agreement for any reason, business associate shall return to covered entity [or, if agreed to by covered entity, destroy] all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.

[Option 2—if the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement]

Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;

3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;
4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and
5. Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

#### **Miscellaneous [Optional]**

(a) [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) [Optional] Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

## **HIPAA Breach Notification Policy**

### **I. PURPOSE AND APPLICABILITY**

The purpose of this Policy is to ensure that \_\_\_\_\_'S breach notification Policy complies with the requirements articulated under HIPAA.

### **II. DEFINITIONS**

A Breach is defined as the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule, or which otherwise compromises the security or privacy of the PHI.

Breach excludes the following:

- Any unintentional acquisition, access, or use of PHI by a Workforce Member or person acting under the authority of a CE or BA, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in a further use or disclosure in a manner not permitted under the Privacy Rule;
- Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person to access PHI at the same CE or 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 prohibited by the Privacy Rule

Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same Ce or 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 prohibited by the Privacy Rule; or

- A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

### **III. REQUIREMENTS**

Absent an applicable exception, an acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule is presumed to be a breach unless the CE or BA, as applicable, has demonstrated a low probability that the PHI has been compromised based on a risk assessment. The assessment must include, at a minimum, these factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of reidentification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether PHI was actually acquired or viewed; and
- The extent to which the risk to PHI has been mitigated.

## **Breach Notification to Individuals**

1. Where \_\_\_\_\_ has discovered that a breach of unsecured PHI has occurred, it must notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of a breach.
2. A CE is deemed to have discovered a breach as of the first day on which such breach is known by the CE, or, would have been known by the CE through the exercise of due diligence. A CE shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person who committed the breach, who is a Workforce Member or agent of the CE.
3. Unless directed otherwise by law enforcement, (in accord with HIPAA §164.412) CE must provide the required notification to affected individuals in writing, without unreasonable delay, and in no case later than 60 calendar days after discovery of a breach.
4. The required notice to an affected individual must be written in plain language and must include, to the extent possible, the following:
  - A brief description of the event, including the date of the breach and the date the breach was discovered, and if known;
  - A description of the unsecured types of PHI involved in the breach (such as whether full names, social security numbers, DOBs, etc. were involved);
  - Any steps that individuals should take to protect themselves from potential harm as a result of the breach;
  - A brief description of the actions that CE is taking to investigate the breach, mitigate harm to individuals, and to protect against any further breaches; and
  - Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.
5. \_\_\_\_\_ must provide the written notice by mailing it via 1st class mail to the last known address of the individual. If the individual had previously agreed to receive notice electronically and such agreement has not been withdrawn, then \_\_\_\_\_ may send the notification via e-mail. The notification may be provided in one or more mailings as information becomes available. If \_\_\_\_\_ is aware that the individual is deceased AND it has the address of a next of kin or personal representative, then it must send the next of kin or the representative the notice via 1st class mail. Depending on \_\_\_\_\_'S factual scenario, additional substitute notice requirements may be applicable. For additional information please consult HIPAA §164.404(d)(2)-(d)(2)(B).
6. In situations deemed by \_\_\_\_\_ to be urgent because of possible imminent misuse of unsecured PHI, it may provide information to affected individuals via telephone or other forms of communication, but it must also still provide the appropriate form of written notice.

### **Breach Notification to the Media**

1. If a breach of unsecured PHI involves the information of more than 500 individuals of a State or jurisdiction, then following the discovery of such breach, \_\_\_\_\_ must notify prominent media outlets serving the State or jurisdiction.
2. Unless directed otherwise by law enforcement, (in accord with HIPAA §164.412) \_\_\_\_\_ must provide the required notification under this Section (II)(a), without unreasonable delay, and in no case later than 60 calendar days after discovery of a breach.
3. The notification required to be provided to the media must include all of the elements required under Section (I)(g).

### **Breach Notification to the Secretary of HHS**

1. \_\_\_\_\_ must notify the Secretary of HHS following the discovery of a breach of unsecured PHI
2. If the breach involves information pertaining to more than 500 individuals then \_\_\_\_\_ must provide notice to the Secretary contemporaneously with the individual notice requirement. \_\_\_\_\_ must provide notice to the Secretary in the manner specified on the HHS website. Please see the overview section of this Policy for a link to the appropriate website.
3. If the breach involves less than 500 individuals then \_\_\_\_\_ must maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the required notice to the Secretary for breaches discovered during the preceding calendar year, consistent with the manner specified on the HHS website.

### **Breach Notification by a Business Associate**

1. A BA must notify a CE following a breach of unsecured PHI.
2. A breach shall be treated as discovered by a BA as of the 1<sup>st</sup> day on which it became known to the BA or, if by exercising reasonable diligence, would have been known to the BA. A BA shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence, would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the BA.
3. Unless directed otherwise by law enforcement under §164.412, a BA must provide the required notice to the CE without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach.
4. To the extent possible, the notice must include the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed during the breach. Additionally, the BA must provide the CE with any other information that the CE is required to include in a notice to an individual as outlined in this Section (I)(g). Such information must be supplied to the CE in accord with the time at which the BA is required to notify the CE of a breach. If at such time, the information is not yet readily available, then the BA must promptly thereafter notify the CE as the information becomes available.



## **Law Enforcement Delay**

1. If a law enforcement official notifies a CE or BA that any notification, notice, or posting required under the Breach Notification Rule would hinder a criminal investigation or harm national security, then the CE or BA must:
  - If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
  - If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement from the official has been submitted within 30 days from the date that the oral statement was made.

## **Administrative Requirements and Burden of Proof**

1. Whether acting as a CE or BA, \_\_\_\_\_ should be aware that the administrative requirements outlined in HIPAA §164.530(b), (d), (e), (g), (h), (i), and (j) are applicable under the Breach Notification Rule.
2. In the event of a use or disclosure in violation of the Privacy Rule, \_\_\_\_\_ as a CE or BA, as applicable, bears the burden of demonstrating that all notifications required under the Breach Notification Rule were complied with, or that any use or disclosure did not constitute a breach as defined under the same rule.

## **IV. RESPONSIBILITY**

1. All Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. This Policy is to be implemented and maintained by the Privacy Officer.

## **V. DOCUMENTATION**

\_\_\_\_\_ must maintain documentation that all required breach notifications were made, or alternatively documentation to demonstrate that notification was not required because (1) it conducted a risk assessment and found a low probability that PHI had been compromised by an impermissible use or disclosure; or (2) any other applicable exception to the definition of “breach” was applicable. \_\_\_\_\_ must maintain copies of the required documentation for a period of six (6) years from the date that such documents were created.

## **VI. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_.

## SAMPLE HIPAA BREACH NOTIFICATION LETTER

[INDIVIDUAL'S NAME]

[STREET ADDRESS]

[CITY, STATE, AND POSTAL CODE]

[DATE]

### HIPAA BREACH NOTIFICATION

Dear [INDIVIDUAL'S NAME]:

We are sending you this letter to inform you of a potential privacy issue involving \_\_\_\_\_.

#### **WHAT HAPPENED AND INFORMATION INVOLVED**

On [DATE OF DISCOVERY], it was discovered that [DESCRIPTION OF INCIDENT AND DATE OF BREACH]. [At this point in time, we have no reason to think that the information has been accessed or used by an unauthorized individual.] [The incident may have involved [THEFT OR OTHER CRIMINAL ACTIVITY] and it was reported to law enforcement officials.] We have learned that your personal information, including [TYPES OF INFORMATION], may have been compromised.

#### **WHAT WE ARE DOING IN RESPONSE**

\_\_\_\_\_ values your privacy and deeply regrets that this incident occurred. \_\_\_\_\_ is conducting an enterprise-wide review of the potentially affected [records/computer system/[OTHER]], and will notify you if there are any significant developments.] \_\_\_\_\_ is also reviewing its HIPAA privacy and security policies and procedures to ensure ongoing compliance with HIPAA's requirements. \_\_\_\_\_ has implemented additional security measures intended to protect the privacy of plan participants and other individuals.

#### **WHAT YOU CAN DO IN RESPONSE**

To protect yourself from potential harm resulting from the breach, you should [DESCRIPTION OF STEPS INDIVIDUALS SHOULD TAKE TO PROTECT THEMSELVES]. In addition, we will make available to you, upon your request, one year of free credit monitoring and reporting services, beginning [DATE OF NOTICE]. You may also choose to contact the three major consumer credit reporting agencies to place a "Fraud Alert" on your credit report.

We understand that this incident may pose an inconvenience to you and regret that the incident has occurred. \_\_\_\_\_ is committed to protecting your personal information, and we want to assure you that we have policies and procedures to protect your privacy.

For further information and assistance [, or if you want to take advantage of the free credit monitoring service], please contact [REPRESENTATIVE} at [TOLL-FREE TELEPHONE NUMBER] or [EMAIL].

Sincerely,

[NAME]

HIPAA Privacy Officer

## The Security Rule

The Security Rule was designed to protect all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form. The Security Rule refers to this information as “electronic protected health information” (e-PHI). The Security Rule does not apply to PHI that is transmitted orally or in writing.

The law was promulgated to be “technologically neutral” so that organizations could adapt to technological changes without fear of falling out of compliance with the Rule. Accordingly, the law does not mandate the use of specific technologies, but rather, it establishes certain **standards that must be met**. In so structuring the Rule, HHS also acknowledged that one size does not fit all, and so the Rule is designed to allow organizations to utilize technologies that best fit their needs while simultaneously ensuring compliance with the Rule. The standards fall into three categories: administrative, physical, and technical safeguards. The following is a list of the standards that are contained within each safeguard.

Administrative Safeguards include: security management processes, assigned security responsibilities, workforce security, information access management, security awareness and training, security incident procedures, contingency planning, evaluation, and business associate agreements and other related contract management

Physical Safeguards include: facility access controls, workstation use, workstation security, and device and media controls

Technical Safeguards include: access, control, audit controls, integrity, person or entity authentication, and transmission security.

Appearing within each standard are implementation specifications. The implementation specifications are either required or addressable. Where an implementation specification is required, \_\_\_\_\_ must implement the specification. Where the implementation specification is addressable, \_\_\_\_\_ (as a CE or BA) must assess whether the specification is a “reasonable and appropriate” safeguard given its specific environment and the likely contribution that such specification will have in protecting e-PHI. If \_\_\_\_\_ deems a specific implementation reasonable and appropriate then it must implement the specification. If, upon review, \_\_\_\_\_ determines that the implementation specification is not reasonable and appropriate then it must document why it would not be reasonable and appropriate to implement the specification, and implement an alternative measure if doing so would be reasonable and appropriate. \_\_\_\_\_ must review and modify the security measures implemented under Subpart C of Part 164 as needed to continue the provision of reasonable and appropriate protection of e-PHI and update documentation of such security measures as required by HIPAA §164.316(b)(2)(iii). \_\_\_\_\_ should also be aware that HIPAA requires that a CE document the rationale behind every security decision. Per HIPAA §164.316, \_\_\_\_\_ must maintain the policies and procedures required under the Security Rule in written (which may be electronic) form. If an action, activity, or assessment is required under the Security Rule to be documented, then it must be maintained in a written record. Any such documentation must be retained for 6 years from the date of its creation or the date when it was last in effect, whichever is later.

# HIPAA Risk Analysis & Management Policy

---

## I. PURPOSE AND APPLICABILITY

\_\_\_\_\_ has created this Policy to comply with the risk analysis and management implementation specifications required under HIPAA §164.308(a)(1)(ii)(A) and §164.308(a)(1)(ii)(B). The purpose of the risk analysis and management implementation specifications, and consequently this Policy, is twofold. First, a risk assessment policy positions \_\_\_\_\_ to better identify and understand where and how it creates, receives, maintains, and transmits e-PHI. With this understanding, \_\_\_\_\_ is better able to determine where potential threats and vulnerabilities exist within its EIRs. Having identified such threats and vulnerabilities allows \_\_\_\_\_ to then identify appropriate security safeguards for reducing and eliminating security risks. Second, once \_\_\_\_\_ has identified applicable and appropriate safeguards, it is better able to establish policies and procedures that can be utilized to implement such safeguards.

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles E-PHI on behalf of \_\_\_\_\_.

## II. PERTINENT BACKGROUND INFORMATION

To better understand risk analysis and risk management processes it is important to be familiar with the terms, vulnerability, threat, and risk, and the relationship between the three. The definitions are as follows:

**Vulnerability** is defined 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 an inappropriate use or disclosure of EPHI.

Vulnerabilities may be grouped into two general categories, technical and non-technical. 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.

**A threat** is “[t]he 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 may include floods, earthquakes, tornadoes, and landslides.

Human threats are enabled or caused by humans and may include 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 and inaccurate data entry) actions.

Environmental threats may include power failures, pollution, chemicals, and liquid leakage.

Note that a threat must have capability to trigger or exploit vulnerability to create risk.

The definition of **risk** is clearer once threat and vulnerability are defined. A risk 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—*

- *Unauthorized (malicious or accidental) disclosure, modification, or destruction of information*
- *Unintentional errors and omissions*
- *IT disruptions due to natural or man-made disasters*
- *Failure to exercise due care and diligence in the implementation and operation of the IT system.”*

Risk is a function of 1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and 2) the resulting impact on the organization. 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.

### III. DETAILED POLICY STATEMENT

#### Risk Analysis Requirements

1. Identify where E-PHI is created, received, maintained, or transmitted.
2. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate. (See Section 164.308 (a)(1)(ii)(A))
3. Consider system capacities, and removable media and portable computing devices such as: laptops, external hard drives, floppy disks, etc.
4. Such an assessment will create an understanding of \_\_\_\_\_’S IT system environment and its boundaries and capacities. Next, develop a list of technical and non-technical system vulnerabilities that may be exploited by potential threat sources.
5. Review \_\_\_\_\_’S own “lived experiences” and other applicable examples from similarly situated entities to help identify a list of potential security threats.

6. Develop a threat list comprised of potential threat sources that could exploit system vulnerabilities.
7. Document and assess the effectiveness of technical and non-technical security measures that have been or will be implemented by \_\_\_\_\_ to reduce the likelihood that a given threat may exploit a system vulnerability.
8. Conduct a likelihood analysis to determine the extent to which harm would result to \_\_\_\_\_ and its patients if a given threat source were to successfully exploit a vulnerability. Assign a likelihood rating for each threat source/vulnerability pair.
9. Conduct an impact analysis by examining the extent to which an adverse impact would occur in the event that a particular threat source successfully exploited a system vulnerability.
10. Weighing the results of the likelihood analysis and impact analysis, determine the degree of risk that is involved under each threat/vulnerability pairing.
11. Based on the determined degree of risk for each threat/vulnerability pairing, \_\_\_\_\_ must identify relevant security measures that can be implemented to limit the exposure of such risks.

### **Risk Management Requirements**

1. The results of the risk assessment must be documented and provided to the SO and \_\_\_\_\_'S owner/s so that they may make a determination as to whether or not \_\_\_\_\_ should implement recommended security measures.
2. Based on the results of the risk assessment, \_\_\_\_\_ must create a prioritized list of actions that need to be addressed. The list should be compiled in a top down fashion and should begin with the threat/vulnerability pairing that presents the greatest risk to \_\_\_\_\_, thus requiring the most immediate attention.
3. Once the list has been compiled, \_\_\_\_\_ must determine the appropriate security measure to implement to address the risk. It is important to understand that HIPAA does not require \_\_\_\_\_ to implement a security measure to address every risk concern. Where a security measure is not a standard or required implementation specification, \_\_\_\_\_ must assess whether implementing such a security measure is reasonable and appropriate given \_\_\_\_\_'S environment, when analyzed with reference to the likely contribution of protecting E-PHI. If \_\_\_\_\_ finds the measure to be reasonable and appropriate then it must implement it. If it is found not to be reasonable and appropriate then it must document the reasons why, and if an alternative measure is appropriate and reasonable, then \_\_\_\_\_ must implement that measure. In determining whether it is "reasonable and appropriate" to implement such security measure, \_\_\_\_\_ must assess:
  - i. The size, complexity, and capabilities of the covered entity or business associate;
  - ii. The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities;
  - iii. The costs of security measures; and

- iv. The probability and criticality of potential risks to electronic protected health information.
4. Taking into consideration all of the information from the above-mentioned steps, the Security officer or his/her designees, must implement the appropriate security measure necessary to reduce risk to information systems and protect the confidentiality, integrity, and availability of E-PHI.

#### **Maintenance**

1. This risk analysis and management policy must be reviewed annually and revised as appropriate. In addition, this Policy must be updated promptly to respond to any significant legislative, environmental, or operational changes.

### **IV. DOCUMENTATION**

1. Any documentation required under this Policy must appear in a written format and be retained for 6 years from the date of its creation or the date when it was last in effect, whichever is later.

### **V. RESPONSIBILITY**

1. The Security Officer is responsible for ensuring the successful implementation, maintenance, and compliance with this Policy.
2. All Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.

### **VI. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.



## HIPAA Information System Activity Review Policy

---

### I. PURPOSE AND APLLICABILITY

\_\_\_\_\_ has implemented this Policy in order to comply with HIPAA §164.308(a)(1)(ii)(D) – the information system activity review implementation specification - which requires \_\_\_\_\_ to regularly review records of information system activity. Accordingly, this Policy has been established to enable and review logs (access logs and audit logs) on electronic information resources (EIRs) that create, receive, maintain, or store e-PHI.

Electronic and information resources include information technology and any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, duplication, or delivery of data or information. The term includes but is not limited to “telecommunications products (such as telephones), information kiosks and transaction machines, World Wide Web sites, multimedia, and office equipment such as copiers and fax machines.”

Some of the ways in which \_\_\_\_\_ might utilize EIRs include, but are not limited to:

- software applications and operating systems
- websites, both Internet and Intranet
- telecommunications products
- video and multimedia products
- self-contained, closed products, such as copiers, printers and fax machines
- desktop and portable computers
- audio and video recordings
- documents such as Microsoft Word, Excel, PowerPoint and PDFs

All Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.

### II. DETAILED POLICY STATEMENT

#### Requirements

\_\_\_\_\_ requires that the following procedures be in place in order to ensure that access and activity is recorded and reviewed for EIRs that create, receive, maintain, or store e-PHI.

1. Logging must be enabled at the server, application/database, and workstation level.

2. Logs must be reviewed whenever there is a suspected or reported security breach on systems containing e-PHI, or as otherwise required by the Security Officer.
3. The Security Officer is charged with establishing the time and manner in which specific logs are to be reviewed.
4. Log review shall include investigation of suspicious activity, and escalation to \_\_\_\_\_'S Security Officer where applicable.

### **Responsibility**

1. All Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. The Security Officer is responsible for the implementation of and adherence to this Policy.
3. No Workforce Member or vendor shall conduct log reviews unless designated to do so by the Security Officer.

### **III. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.

# HIPAA Sanction Policy

---

## I. PURPOSE AND APPLICABILITY

The purpose of this policy is to apply appropriate sanctions against workforce members who fail to comply with the privacy and security practices, policies, and procedures of \_\_\_\_\_. This Policy is designed to meet the requirements articulated under HIPAA §164.308(a)(1)(ii)(C) pertaining to the Security Rule, as well as, HIPAA §164.530(e)(1) which pertains to the Privacy Rule. This Policy applies to all types of PHI, including: oral, written, and electronic.

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles E-PHI on behalf of \_\_\_\_\_.

## II. DEFINITIONS

This Policy categorically defines the unpermitted use or disclosure of PHI by a Workforce Member into the following 3 categories based on the egregiousness of the act:

### **Category 1:** Improper and/or unintentional disclosure of PHI

Examples of this type of disclosure include but are not limited to:

- Accessing information that is not necessary for you to do your job;
- Sharing your computer access codes (user name & password);
- Leaving your computer unattended while logged in to a PHI program;
- Sharing PHI with another Workforce Member without authorization;
- Making copies of PHI without authorization;
- Making unauthorized changes to PHI;
- Leaving a copy of a patient's PHI in a public area; or
- Discussing a patient's PHI in a public area where it might be overheard by a \_\_\_\_\_ customer.

### **Category 2:** Intentional and unauthorized accessing of PHI

Examples of this type of disclosure include but are not limited to:

- Accessing/ reviewing a patient's record out of curiosity or concern;
- Using another Workforce Member's computer login information;
- Improperly accessing the record of a friend, relative, or Workforce Member; or
- Failure to comply with a corrective action.

### **Category 3:** Intentional and unauthorized disclosures of PHI

Examples of this type of disclosure include but are not limited to:

- Obtaining PHI through false pretenses;
- The unauthorized use or disclosure of PHI for commercial/personal gain, or malicious intent; or
- The repeated offense of a Category 1 or 2 offense;

### **III. DETAILED POLICY STATEMENT**

#### **Requirements**

1. Any and all Workforce Members must be disciplined for violating this Policy, no exceptions.
2. All Workforce Employees must sign a form of acknowledgment stating that they have read and agree to abide by the procedures set forth in this Policy.
3. In the event that \_\_\_\_\_ makes changes to this Policy, then all Workforce Members must sign an acknowledgement stating that they have been made aware of, and agree to abide by, the updated policy.
4. Where the violation includes a Category 1 offense, appropriate disciplinary steps are to include at least one of the following: verbal reprimand; written reprimand to be retained in the Workforce Member's personnel file; undergoing additional HIPAA training; and/or undergoing additional training pertaining to \_\_\_\_\_'S policies and procedures pertaining to the Privacy and Security Rules.
5. Where the violation includes a Category 2 offense, appropriate disciplinary steps are to include at least one of the following: verbal reprimand; written reprimand to be retained in the Workforce Member's personnel file; undergoing additional HIPAA training; undergoing additional training pertaining to \_\_\_\_\_'S policies and procedures pertaining to the Privacy and Security Rules; and/or other corrective action potentially including suspension or termination of employment.
6. Where the violation includes a Category 3 offense, appropriate disciplinary steps are to include the termination of employment.
7. Any time a disciplinary action is taken against a Workforce Member, such action must be documented in a written statement (which may be in electronic form).
8. Retaliation is strictly prohibited. Neither \_\_\_\_\_ nor any Workforce member thereof, shall intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against:

#### **Any individual or other person for:**

- Filing a complaint with HHS;
- Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under HIPAA Part 160; or
- Opposing any unlawful act or practice, provided that:

- The individual or other person (including a \_\_\_\_\_ employee) has a good faith belief that the act or practice being opposed is unlawful; and
  - The manner of such opposition is reasonable and does not involve use or disclosure of an individual's protected information in violation of DHH policy.
9. Nothing in this Policy shall prevent a Workforce Member or Business Associate from disclosing PHI in instances in which the Workforce Member/BA is acting as a whistleblower or has been the victim of a crime provided the following has been met:

Regarding whistleblowing, the Workforce Member/BA must believe in good faith that \_\_\_\_\_ has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services or conditions provided by \_\_\_\_\_ could endanger one or more of \_\_\_\_\_'S patients, workforce members, or the public; and

The disclosure is made to:

- An oversight agency or public authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of \_\_\_\_\_;
  - An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or of misconduct by \_\_\_\_\_; or
  - An attorney retained by or on behalf of the \_\_\_\_\_ Workforce Member or BA for the purpose of determining the legal options of the Workforce Member or BA with regard to potential actions that might be taken as a whistleblower.
10. A Workforce Member who is the victim of a criminal act may disclose PHI to law enforcement provided that the PHI disclosed is about the suspected perpetrator of the criminal act, and the PHI disclosed is limited to the following types: name and address, date and place of birth, social security number, ABO blood type and Rh factor, type of any injury, date and time of any treatment, and the date and time of death if applicable.

#### **IV. RESPONSIBILITY**

1. All Workforce Members, BAs, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. This Policy is to be implemented and maintained by the Privacy Officer and Security Officer.

#### **V. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_, or the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.

## **HIPAA Workforce Security Policy**

### **I. PURPOSE AND APPLICABILITY**

The purpose of this Policy is to implement procedures to ensure that all of \_\_\_\_\_'S Workforce Members have appropriate access to E-PHI, and to prevent those Workforce Members who do not have authorization to E-PHI from accessing such information as required by the Workforce Security standard found at §164.308(a)(3)(i).

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles E-PHI on behalf of \_\_\_\_\_.

### **II. DETAILED POLICY STATEMENT**

#### **Requirements**

1. The Security Officer must establish and implement policies and procedures to ensure that \_\_\_\_\_'S Workforce Members have access to E-PHI only as necessary to complete their job functions.
2. Per implementation specification §164.308(a)(3)(ii)(A), the SO must implement procedures for the authorization and/or supervision of Workforce Members who work with E-PHI or in locations where it might be accessed.
3. Per implementation specification §164.308(a)(3)(ii)(B), the SO must adopt procedures to address Workforce clearance. The purpose of this specification is to ensure that \_\_\_\_\_ has implemented procedures to determine that the access of E-PHI by a Workforce member is appropriate.
4. Per implementation specification §164.308(a)(3)(ii)(C), the SO must implement termination procedures so that access to E-PHI by a Workforce Member/BA is restricted whenever such a "person's" job duties change or their employment ends.

### **III. RESPONSIBILITY**

1. All Workforce Members, management, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. In the event that \_\_\_\_\_ works with a Business Associate, the Business Associate must have substantially similar policies and procedures in place, and those procedures must satisfy all of the requirements expressed under the Security Rule.
3. This Policy is to be implemented and maintained by the Security Officer.

### **IV. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.

# HIPAA Information Access Management Policy

---

## I. PURPOSE AND APPLICABILITY

The purpose of this Policy is to implement procedures to ensure that \_\_\_\_\_ has implemented policies and procedures for authorizing access to E-PHI as required by the Information Access Management standard found at §164.308(a)(4)(i).

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles E-PHI on behalf of \_\_\_\_\_.

## II. DETAILED POLICY STATEMENT

### Requirements

1. The SO is responsible for implementing policies and procedures that authorize Workforce Members/ BAs to access E-PHI.
2. Per implementation specification §164.308(a)(4)(ii)(B), the SO must implement access authorization policies and procedures to ensure that access to E-Phi and the devices on which it is housed, are accessed only by properly authorized Workforce Members/BAs.
3. Per implementation specification §164.308(a)(4)(ii)(C), the SO must, based upon \_\_\_\_\_'S access authorization policies and procedures, create a policy that establishes, documents, reviews, and modifies a user's right of access to a workstation, program, transaction, or process that contains E-PHI.

## III. RESPONSIBILITY

1. All Workforce Members, management, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. In the event that \_\_\_\_\_ works with a Business Associate, the Business Associate must have substantially similar policies and procedures in place, and those procedures must satisfy all of the requirements expressed under the Security Rule.
3. This Policy is to be implemented and maintained by the Security Officer.

## IV. DOCUMENTATION

The documentation required by this Policy must appear in written form (which may be electronic) and be retained for a period of 6 years from the date of its creation or the date when it was last in effect, whichever is later.

## V. GETTING HELP

For questions about this policy, or to escalate an issue, please contact the Security Officer at \_\_\_\_\_ or \_\_\_\_\_, or the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_.

## HIPAA Facility Access Controls Policy

---

### I. PURPOSE AND APPLICABILITY

The purpose of this Policy is to ensure that \_\_\_\_\_ has sufficient facility access controls in place to comply §164.310(a)(1) and the facility access controls standard.

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles E-PHI on behalf of \_\_\_\_\_.

### II. DETAILED POLICY STATEMENT

#### Requirements

1. The SO is responsible for developing and implementing policies and procedures that limit physical access to electronic information systems and the facility or facility in which they are housed, while ensuring that properly authorized access is allowed. The SO must also implement procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
2. The SO must implement facility access controls that are appropriate to protect facility access in light of \_\_\_\_\_'S specific operating environment. A non-exhaustive list of appropriate procedures that \_\_\_\_\_ might implement includes ensuring that:
  - All restricted areas have visible warning signs alerting the general public that such areas are off limits;
  - All restricted areas are locked and accessible only to authorized Workforce Members;
  - All restricted areas of \_\_\_\_\_'S operation should be under 24/7 video surveillance;
  - Workforce Members are to wear standard issued identification badges at all times while on \_\_\_\_\_ premises;
  - If a Workforce member loses his/her badge then he/she should notify the Security officer. If the badge contains an electronic keycard or other similar electronic data, then the Security Officer must immediately deactivate the badge to ensure that \_\_\_\_\_'S facility operations are not compromised;
  - When a Workforce Member's employment ends or job duties change, the Security Officer must respond appropriately by deactivating or adjusting, as the case may be, the Workforce Member's badge;
  - A means for monitoring and reviewing a Workforce Member's physical access to systems and locations that contain E-PHI;



- Business Associates do not access restricted areas unless accompanied by an authorized Workforce member;
  - A Business Associate must provide acceptable proof of identity prior to being escorted to a restricted area;
  - Anytime a Business Associate accesses electronic systems or physical systems of \_\_\_\_\_, the event must be logged. The log must contain the time, place, person, and reason for the access. The documentation must be written and may be stored in electronic form;
  - The Security Officer must have the ability to immediately prevent access to any and all forms of EIRs; and
  - Anytime physical repairs or modifications are made to the physical components of the facility for security purposes – such changes might include alterations to hardware, locks, doors, walls, etc. - such changes must be documented in written form.
3. The SO must ensure that access control is predicated on user identification authentication.
  4. The So must establish a line of authority for granting access to \_\_\_\_\_'S facility and the systems on which E-PHI is stored.

### **III. RESPONSIBILITY**

1. All Workforce Members, Business Associates, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. The Security Officer is responsible for implementing and maintaining this Policy.

### **IV. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.

## **HIPAA Access Control Policy**

---

### **I. PURPOSE AND APPLICABILITY**

The purpose of this Policy is to ensure that \_\_\_\_\_ has sufficient technical access controls in place to comply §164.312(a)(1) the access control standard.

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles E-PHI on behalf of \_\_\_\_\_.

### **II. DETAILED POLICY STATEMENT**

#### **Requirements**

1. The SO is responsible for implementing technical policies and procedures for electronic information systems (EIRs) that maintain E-PHI to allow access only to those persons or software programs that have been granted access rights.
2. The SO is responsible for assigning a unique name and/or number for identifying and tracking user identity.
3. The SO must take reasonable steps to ensure the integrity of all EIRs. Appropriate steps might include the installation of encryption software, anti-virus software, utilizing automatic logoff processes when an EIR has not been in use for a predetermined amount of time, etc.
4. The SO must also develop and implement an emergency access procedure to ensure that authorized Workforce Members have access to E-PHI during emergencies.
5. The SO is responsible for developing audit controls; i.e., procedural mechanisms that record and examine activity in information systems that contain or use E-PHI.
6. The SO must also implement policies and procedures pertaining to data integrity. Namely, the SO must ensure that policies and procedures exist to protect E-PHI from unauthorized alteration and/or destruction.
7. In order to ensure that E-PHI is not improperly altered or destroyed, the SO must implement authentication policies and procedures in order to verify and confirm that access to E-PHI and the systems on which it is stored is legitimate.
8. The SO must ensure that proper procedures exist to verify that the person or entity requesting access to E-PHI is in fact the individual/entity in question.
9. The SO must ensure that proper transmission procedures are in place in order to preserve the integrity of E-PHI when it is being transmitted over an electronic network.

### **III. RESPONSIBILITY**

1. All Workforce Members, Business Associates, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. The Security Officer is responsible for implementing and maintaining this Policy.

### **IV. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.

## HIPAA Facility Security Plan Policy

---

### I. PURPOSE AND APPLICABILITY

The purpose of this Policy is to ensure that \_\_\_\_\_ has a facility security plan in place, as required by §164.310(a)(1)(2)(ii).

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles E-PHI on behalf of \_\_\_\_\_.

### II. DETAILED POLICY STATEMENT

#### Requirements

1. The SO is responsible for implementing policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
2. The SO will ensure that \_\_\_\_\_ restricts facility access by Workforce Members and BAs to only those areas in which said individuals require access to fulfill their job duties. Accordingly, physical access to particular areas within \_\_\_\_\_, will be restricted by keycard access.
3. The SO will ensure that \_\_\_\_\_'S operations are under video surveillance 24/7.
4. All Workforce Members/BAs are responsible for reporting any suspicious activities regarding the security of PHARMCY'S premises to the SO.
5. The SO must ensure \_\_\_\_\_ has a proper closing procedure in place, in order to protect against unlawful entry during non-business hours.
6. If a Workforce Member or BA ever loses his/her security badge, then the SO must take immediate action to deactivate said badge in order to preserve the integrity of \_\_\_\_\_'S operations.

### III. RESPONSIBILITY

1. All Workforce Members, Business Associates, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. The Security Officer is responsible for implementing and maintaining this Policy.

### IV. GETTING HELP

For questions about this policy, or to escalate an issue, please contact the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.

## HIPAA Facility Security Maintenance Records Policy

---

### I. PURPOSE AND APPLICABILITY

The purpose of this Policy is to ensure that \_\_\_\_\_ has a facility security plan in place, as required by §164.310(a)(1)(2)(iv).

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles E-PHI on behalf of \_\_\_\_\_.

### II. DETAILED POLICY STATEMENT

#### Requirements

1. The SO must implement policies and procedures to document repairs and modifications to the physical components of \_\_\_\_\_'S facility which are related to security (for example, hardware, doors, locks, etc.).
2. The SO must create and maintain a facility security log book. Any time a repair or modification to \_\_\_\_\_'S facility is facilitated for security purposes; the SO must document the event in the log book.
3. The log book should document the time, date, change, and rationale for the change.

### III. RESPONSIBILITY

1. All Workforce Members, Business Associates, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. All BAs must have a similar policy in place.
3. The Security Officer is responsible for implementing and maintaining this Policy.

### IV. DOCUMENTATION

1. Any time \_\_\_\_\_ repairs or modifies its facility for security purposes, it must document the event. The documentation must be retained for a period of six (6) years.

### V. GETTING HELP

For questions about this policy, or to escalate an issue, please contact the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.

## HIPAA Workstation Use & Security Policy

---

### I. PURPOSE AND APPLICABILITY

The purpose of this Policy is to ensure that \_\_\_\_\_ has a workstation use and security policy in place to comply with the requirements of §164.310(b) and §164.310(c).

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles E-PHI on behalf of \_\_\_\_\_.

### II. DETAILED POLICY STATEMENT

#### Requirements

1. The SO must implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access E-PHI.
2. All Workforce Members and BAs are to use \_\_\_\_\_ workstations for official \_\_\_\_\_ business only. No Workforce Member shall be permitted to modify hardware or software configurations or copy/transport software for personal use without prior approval from the Security Officer or his or her designee.
3. When accessing E-PHI, all Workforce Members and BAs shall access only that information which is necessary for them to fulfill their job duties.
4. Consistent with its log policy, \_\_\_\_\_ must continually monitor log and monitor user access to E-PHI systems/workstations. Consequently, the SO must ensure that each Workforce Member/BA is given a unique log-in identifier so that workstation use can be tracked.
5. The SO must ensure that each workstation is locked and accessible only via secure password. Unattended terminals shall be automatically logged off after a period of inactivity. If auto-lockout is not enabled on the terminal, users shall log off before leaving a terminal unattended to help maintain physical security.
6. The SO must take reasonable steps to ensure that workstations containing E-PHI are kept out of public view.
7. The SO must make sure that all workstations containing E-PHI use data encryption software. The SO must also ensure that all workstations are equipped with some form of anti-virus software.
8. No workstation may leave \_\_\_\_\_'S facility unless the SO expressly so authorizes.
9. Workforce Members and BAs are expressly prohibited from copying, transmitting, storing, distributing, or otherwise using E-PHI unless their job duties so demand. Under no circumstances should a Workforce Member or BA use floppy disks, external hard drives, or any other means to backup E-PHI unless the SO specifically tells them to do so.

10. The SO must ensure that proper policies and procedures are in place to restrict a Workforce Member/BAs access to workstations that contain E-PHI in instances involving termination of employment/contract or whenever a change in one's job duties affects the need to access E-PHI.
11. All Workforce Members and BAs have an affirmative duty to notify the Security Officer or Privacy Officer if they suspect that a workstation's security has been compromised.

### **III. RESPONSIBILITY**

1. All Workforce Members, Business Associates, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. The Security Officer is responsible for implementing and maintaining this Policy.

### **IV. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.

## HIPAA Contingency Plan Policy

---

### I. PURPOSE AND APPLICABILITY

The purpose of this Policy is to ensure that \_\_\_\_\_ has the proper procedures in place to adequately respond to an emergency or other occurrence (for example, fire, vandalism, system failure, natural disaster) that causes damage to systems that contain E-PHI. This Policy is required to comply with the requirements of §164.308(a)(7).

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles E-PHI on behalf of \_\_\_\_\_.

### II. DETAILED POLICY STATEMENT

#### Requirements

1. The Security Officer must develop a contingency plan which will allow for the recovery of E-PHI in the event that the systems and facilities which store such data become destroyed or damaged.
2. The plan must establish a line of succession to ensure that proper decision-making authority remains uninterrupted in the event that the plan must be activated.
3. The Security Officer is the first individual charged with ensuring proper execution of the plan. If the Security officer is unable/unavailable to perform the required duties, then the Privacy Officer must fill his/her shoes. If the Privacy Officer is also unable to perform the duties required under the plan, then another team member who has been properly trained on the disaster response procedures required under the plan, shall assume responsibility for properly executing the plan.
4. The Security Officer shall establish criteria for validation/testing of the Contingency plan, an annual test schedule, and ensuring implementation of the test.
5. Contingency plan testing shall occur on at least an annual basis. When a contingency plan test reveals flaws and/or area where \_\_\_\_\_ can improve, then \_\_\_\_\_'S SO must make appropriate revisions to the plan.
6. The validation/testing exercises must comply with the standards articulated in the most recent version of the Risk Management Handbook (RMH). The chapter on Contingency Planning of the handbook can be found here:  
<https://www.cms.gov/Research.../CMS.../RMH-Chapter-6-Contingency-Planning.pdf>
7. Once \_\_\_\_\_ becomes aware of a disruption that might have caused damage to systems or facilities that house E-PHI, it must engage in a damage assessment.
8. Damage assessment procedures should include: activities to determine the cause of disruption; the potential for additional disruption; affected physical areas the status of physical infrastructures; the status of IT equipment functionality and inventory, including items that will require replacement; and the estimated time that will be required to repair services to normal operation.



9. When the damage assessment has been completed, the results need to be evaluated to determine whether the Contingency Plan needs to be activated.
10. In the event the Contingency Plan must be activated, \_\_\_\_\_'S top priority must be protecting the health and safety of its staff.
11. In addition to the above, the Security Officer must ensure that the Contingency Plan adequately contains procedures that allow for: data backup capabilities that can retrieve exact copies of E-PHI, a disaster recovery plan that can restore the loss of data, an "emergency mode operation plan" which will enable \_\_\_\_\_ to continue critical business processes related to protecting the security of E-PHI while operating in emergency mode, and assess the relative critical importance of specific applications and data in support of other contingency plan components. For an example of appropriate procedures to implement, please see the below:
  - **Data Backup Plan – Procedures to Create and Maintain Retrievable Exact Copies of ePHI**
    - Data on each server shall be backed up and accessible
      - \_\_\_\_\_ shall ensure that all critical information on each server has redundant copies stored in different servers, or other appropriate backup methods, at any time.
      - \_\_\_\_\_ shall endeavor to maintain servers in different geographic regions to prevent localized emergencies from disrupting service.
    - Data shall be backed up for long-term storage in case of disaster
      - \_\_\_\_\_ shall create daily long-term backups on all new information on durable media that are disconnected from any network.
      - \_\_\_\_\_ shall store these long-term backups in a safe that protects them from unauthorized access, fire, water/humidity, changes in environment, and any outside force that could cause their premature deterioration.
      - \_\_\_\_\_ shall endeavor to maintain the long-term backup copies of data offsite, to prevent them from being destroyed in a common disaster.
    - Data may be backed up by vendors or on cloud servers
      - \_\_\_\_\_ may use a vendor to outsource data backup so long as the vendor complies with all applicable laws, regulations, and policies.
      - \_\_\_\_\_ cannot delegate liability for security or privacy breaches and is ultimately responsible for the conduct of its vendors.
      - \_\_\_\_\_ shall not merely rely on the representations of vendors without verifying their data backup procedures and contractually obligating them to meet all legal requirements in a Business Associate Agreement.
      - \_\_\_\_\_ may store data in cloud servers so long as the cloud servers comply with all applicable laws, regulations, and policies. \_\_\_\_\_ cannot delegate liability for security or privacy breaches.
      - \_\_\_\_\_ shall contractually obligate cloud computing services vendors by a Subcontractor Business Associate

Agreement which obligates such vendors to meet all legal requirements, and \_\_\_\_\_ shall verify that such vendors' procedures in fact do comply with \_\_\_\_\_'s policies.

- \_\_\_\_\_ may, in its reasonable business judgment, use any process or media so long as such process or media complies with all applicable laws, regulations, and policies, and is considered among the best practice of the information technology industry. All data stored in the cloud shall be Encrypted.
- **Disaster Recovery Plan/Emergency Mode Operation – Procedures to Restore Any Loss of Data and Procedures to Enable Continuation of Critical Business Processes for The Protection of the Security of ePHI While Operating in an Emergency Mode**
  - Access controls shall be in place to enable \_\_\_\_\_ to continue to operate and/or recover lost data in the event of fire, vandalism, natural disaster, or system failure. \_\_\_\_\_ shall document plans that include all necessary information to continue processing following system downtime or a loss of data.
  - Plans shall be maintained at \_\_\_\_\_'s facility.
  - \_\_\_\_\_ shall complete initial and periodic testing of the plans.
  - \_\_\_\_\_ disaster plans shall ensure that critical services remain operational even during and after a disaster.
  - \_\_\_\_\_ should endeavor to maintain redundant servers or data systems in multiple geographic regions to prevent interruptions in service.
  - \_\_\_\_\_ shall stay abreast of developments in the information technology industry that provide for increased data security and implement any best practices that comply with all applicable laws, regulations, and policies.]

### **III. RESPONSIBILITY**

1. All Workforce Members, Business Associates, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. The Security Officer is responsible for implementing and maintaining this Policy.

### **IV. DOCUMENTATION**

\_\_\_\_\_ must provide written documentation of the Contingency Plan, including any changes made to it. In the event that \_\_\_\_\_ must ever activate the Contingency Plan then it should document the event, its responses, and the outcome. All such documentation must be maintained for the requisite statutory period (6 years from the date created or modified, whichever is longer). Further, \_\_\_\_\_ must document the results of any contingency plan tests and any suggested revisions.

### **V. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.

# HIPAA Workforce Training Policy

---

## I. PURPOSE AND APPLICABILITY

The purpose of this Policy is to implement procedures to ensure that all of \_\_\_\_\_'S Workforce Members have appropriate access to E-PHI, and to prevent those Workforce Members who do not have authorization to E-PHI from accessing such information.

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles E-PHI on behalf of \_\_\_\_\_.

## II. DETAILED POLICY STATEMENT

1. HIPAA training is required under §164.308(a)(5) of the Security Rule and also under §164.530(b)(1).
2. \_\_\_\_\_ must require all Workforce members (including management) to participate in the training.
3. The training must cover all of \_\_\_\_\_'S HIPAA policies and procedures. In addition, the training must provide an overview of the HIPAA regulations, including but not limited to, the Privacy Rule, the Security Rule and the Breach Notification Rule.
4. The Security Rule requires security awareness training. Unless unreasonable and inappropriate, the program must include: periodic security reminders/updates, and procedures to address protections from malicious software, login monitoring, and password management.
5. All \_\_\_\_\_ Workforce Members are required to complete \_\_\_\_\_'S HIPAA training program within 30 days of hire and annually thereafter. Further, any time a Workforce Member's job duties change, \_\_\_\_\_ must ensure that the Workforce Member completes \_\_\_\_\_'S HIPAA training.

## III. RESPONSIBILITY

1. All Workforce Members, management, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. In the event that \_\_\_\_\_ works with a Business Associate, the Business Associate must have substantially similar policies and procedures in place, and those procedures must satisfy all of the training requirements expressed under HIPAA.
3. This Policy is to be implemented and maintained by the Privacy Officer.

## IV. DOCUMENTATION

HIPAA requires \_\_\_\_\_ to document its HIPAA training program. A properly documented training program will include the time and date of the training, the test results of the training (if applicable), and the signature of the specific Workforce Member

and Privacy Officer attesting to the completion of the training. The documentation is required to be retained for 6 years from the date of its creation or the date when it was last in effect, whichever is longer.

## **V. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_.

# HIPAA Security Incident Policy

---

## I. PURPOSE AND APPLICABILITY

The purpose of this Policy is to implement a set of procedures that must be followed in the event of a security incident. This Policy is required under HIPAA §164.308(a)(6)(i).

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles E-PHI on behalf of \_\_\_\_\_.

## II. DETAILED POLICY STATEMENT

### Requirements

1. The Security Officer shall be responsible for maintaining \_\_\_\_\_ wide operational IT security situational awareness, and determining the overall security risk posture of \_\_\_\_\_.
2. The Security Officer shall establish and maintain IT security and privacy incident response capabilities, or ensure that incident response capabilities are performed on behalf of \_\_\_\_\_.
3. Whenever a Workforce Member, Business Associate, or other individual who works with \_\_\_\_\_'S E-PHI knows or suspects that a security incident has occurred, said individual must immediately notify the Security Officer. If the Security Officer is unavailable then the Workforce Member, Business Associate, or other individual, shall use best efforts to notify the Privacy Officer or a \_\_\_\_\_ supervisor of the situation.
4. Any reporting of E-PHI related IT security and privacy incidents should be reported in accordance with the reporting guidance specified in US-CERT and NIST SP 800-61 (as amended), Computer Security Incident Handling Guide. For additional information please refer to the following website:

<https://www.us-cert.gov/report>

To access a template for reporting incidents please refer to the following link:

<https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>

5. Following the reporting of a known or suspected security incident involving E-PHI, the Security Officer or another at his/her direction, must run a data analysis and/or forensics examination of the affected system/s on which the E-PHI is created, used, stored, or transmitted.
6. Pending the results of the analysis/forensic examination, the Security Officer must determine whether the integrity/confidentiality of any E-PHI was compromised.
7. If any E-PHI is compromised, then the Security Officer must take corrective action, to the extent practicable, to mitigate any resulting damage.
8. The Security Officer must then provide written documentation of the security incident and the outcome of such incident. The documentation must be retained for the

requisite statutory period; please consult the Statutory Overview section of the Security Rule for additional information.

### **III. RESPONSIBILITY**

1. All Workforce Members, Business Associates, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. The Security Officer is responsible for implementing and maintaining this Policy.

### **IV. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.

# HIPAA Contingency Plan Policy

---

## I. PURPOSE AND APPLICABILITY

The purpose of this Policy is to ensure that \_\_\_\_\_ has the proper procedures in place to adequately respond to an emergency or other occurrence (for example, fire, vandalism, system failure, natural disaster) that causes damage to systems that contain E-PHI.

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles E-PHI on behalf of \_\_\_\_\_.

## II. DETAILED POLICY STATEMENT

### Requirements

1. The Security Officer must develop a contingency plan which will allow for the recovery of E-PHI in the event that the systems and facilities which store such data become destroyed or damaged.
2. The plan must establish a line of succession to ensure that proper decision-making authority remains uninterrupted in the event that the plan must be activated.
3. The Security Officer is the first individual charged with ensuring proper execution of the plan. If the Security officer is unable/unavailable to perform the required duties, then the Privacy Officer must fill his/her shoes. If the Privacy Officer is also unable to perform the duties required under the plan, then another team member who has been properly trained on the disaster response procedures required under the plan, shall assume responsibility for properly executing the plan.
4. The Security Officer shall establish criteria for validation/testing of the Contingency plan, an annual test schedule, and ensuring implementation of the test.
5. Contingency plan testing shall occur on at least an annual basis.
6. The validation/testing exercises must comply with the standards articulated in the most recent version of the Risk Management Handbook (RMH). The chapter on Contingency Planning of the handbook can be found here:  
  
<https://www.cms.gov/Research.../CMS.../RMH-Chapter-6-Contingency-Planning.pdf>
7. Once \_\_\_\_\_ becomes aware of a disruption that might have caused damage to systems or facilities that house E-PHI, it must engage in a damage assessment.
8. Damage assessment procedures should include: activities to determine the cause of the disruption; the potential for additional disruption; affected physical areas and the status of physical infrastructures; the status of IT equipment functionality and inventory, including items that will require replacement; and the estimated time that will be required to repair services to normal operation.

9. When the damage assessment has been completed, the results need to be evaluated to determine whether the Contingency Plan needs to be activated.
10. In the event the Contingency Plan must be activated, \_\_\_\_\_'S top priority must be protecting the health and safety of its staff.
11. In addition to the above, the Security Officer must ensure that the Contingency Plan adequately contains procedures that allow for: data backup capabilities that can retrieve exact copies of E-PHI, a disaster recovery plan that can restore the loss of data, an "emergency mode operation plan" which will enable \_\_\_\_\_ to continue critical business processes related to protecting the security of E-PHI while operating in emergency mode, and assess the relative critical importance of specific applications and data in support of other contingency plan components.

### **III. RESPONSIBILITY**

1. All Workforce Members, Business Associates, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. The Security Officer is responsible for implementing and maintaining this Policy.

### **IV. DOCUMENTATION**

\_\_\_\_\_ must provide written documentation of the Contingency Plan, including any changes made to it. In the event that \_\_\_\_\_ must ever activate the Contingency Plan then it should document the event, its responses, and the outcome. All such documentation must be maintained for the requisite statutory period (6 years from the date created or modified, whichever is longer).

### **V. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.



## HIPAA PHI Data Disposal Policy

---

### I. PURPOSE AND APPLICABILITY

The purpose of this Policy is to ensure that \_\_\_\_\_ has the proper procedures in place to dispose of PHI in a HIPAA compliant manner. The following code sections are pertinent to this discussion: (1) §164.530(c)(1) and (c)(2)(i) makes clear that the \_\_\_\_\_ must have appropriate administrative, technical, and physical safeguards in place to protect all forms of PHI from intentional and unintentional uses and disclosures, and §164.310(d)(2)(i) and (ii) make clear that the \_\_\_\_\_ needs to have procedures that address the disposal of E-PHI and/or the hardware or electronic media on which it is stored. Accordingly, this policy addresses the proper procedures to follow when disposing of paper records of PHI, E-PHI and/or the hardware or electronic media on which it is stored.

This Policy is applicable to all Workforce Members, BAs, and anyone else who handles E-PHI on behalf of \_\_\_\_\_.

### II. DETAILED POLICY STATEMENT

#### Paper Record PHI Disposal Requirements

1. \_\_\_\_\_ must review its own circumstances to determine what steps are reasonable to safeguard PHI through disposal, and implement policies and procedures to carry out those steps.
2. Failure to implement reasonable safeguards can result in impermissible disclosures of PHI. Consequently, \_\_\_\_\_ cannot simply abandon PHI or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons.
3. Appropriate methods for disposing of paper records of PHI include, but are not limited to: shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed. Appropriate methods for disposing of labeled prescription bottles and other PHI is to maintain them in opaque bags in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.4. \_\_\_\_\_ must ensure that any PHI records that are subject to retention requirements are managed carefully so as not to expose PHI while in use, storage, or transportation. This rule applies to all forms of PHI, i.e., E-PHI and the electronic media on which it is stored.
4. Workforce Members must not destroy, alter, or discard any PHI records which are the subject of a subpoena, audit, search warrant, or other investigatory proceeding which legally bars the records from being destroyed. This rule applies to all forms of PHI, i.e., E-PHI and the electronic media on which it is stored.
5. \_\_\_\_\_ must limit access to physical storage rooms that house paper records of PHI to only those Workforce Members who require access to perform their job duties. Any such PHI storage room must be secured by lock and key. This

rule applies to all forms of PHI, i.e., E-PHI and the electronic media on which it is stored.

6. To the extent that \_\_\_\_\_ utilizes “shredding” to destroy paper records of PHI, any records awaiting shredding must be stored in locked containers prior to transport and/or disposal.
7. \_\_\_\_\_ may contract with a Business Associate to dispose of PHI, but the Business Associate must provide adequate assurances that it will use appropriate safeguards when disposing of the PHI, and as always, a Business Associate agreement must be in place.

### **E-PHI Record Disposal Requirements**

1. When disposing of E-PHI or the hardware/electronic media on which it is stored, \_\_\_\_\_ must comply with the Special Publication 800-88, Revision 1, Guidelines for Media Sanitization issued by the National Institute of Standards and Technology (NIST). <https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final>
2. The publication provides three sanitization methods for disposing of E-PHI or the hardware/electronic media on which it is stored. The three methods are: clearing, purging, and destroying. Clearing involves using software or hardware products to overwrite media with non-sensitive data, purging involves degaussing/exposing the media to strong magnetic fields in order to destroy data that is contained in devices that utilize magnetic storage, and destroying involves disintegrating, pulverizing, melting, incinerating, or shredding the hardware/media.
3. Disposal of E-PHI and/or devices on which it is stored is not a one size fits all endeavor. When determining which disposal method should be utilized, \_\_\_\_\_ must consider factors such as: whether the entire hardware/media will be disposed of vs. merely a subset of E-PHI data contained therein, the cost-effectiveness of clearing/purging E-PHI vs. destroying it, whether the hardware/media will be re-used or recycled, and whether other organizations/individuals will have access or control over the hardware/media on which E-PHI has been stored, as may be the case in instances where \_\_\_\_\_ must return leased equipment, or chooses to donate old equipment.
4. As with paper record copies of PHI, \_\_\_\_\_ must ensure that any E-PHI records or the hardware/media on which they are stored, that are subject to retention requirements, are managed carefully so as not to expose PHI while in use, storage, or transportation.
5. Workforce Members must not destroy, alter, or discard any E-PHI records or hardware/media which are the subject of a subpoena, audit, search warrant, or other investigatory proceeding which legally bars the records from being destroyed.
6. To the extent that \_\_\_\_\_ stores hardware/media that contains E-PHI for future sanitization, it must ensure that access is restricted to only those Workforce Members who have a legitimate business purpose for accessing the information. This means that \_\_\_\_\_ should have proper access controls in place, such as a locked storage room.
7. \_\_\_\_\_ may contract with a Business Associate to dispose of E-PHI or the hardware/media on which it is stored, but the Business Associate must provide

adequate assurances that it will use appropriate safeguards when disposing of the PHI, and as always, a Business Associate agreement must be in place.

8. The SO must ensure that \_\_\_\_\_ remains accountable for E-PHI. This means that the SO must develop procedures to maintain and record the movements of hardware and electronic media. In addition, the SO should document the person responsible for keeping track of specific pieces of hardware/electronic media.

### **III. RESPONSIBILITY**

1. All Workforce Members, Business Associates, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. The Compliance Officer and the Security Officer should work together to ensure that all forms of PHI are disposed of properly.

### **IV. DOCUMENTATION**

1. Any time \_\_\_\_\_ disposes of PHI it must document the disposal by filing out a Certificate of Sanitization form. The documentation must be retained for a period of six (6) years.

### **V. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_, or the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.

## **HIPAA Device and Media Controls Policy**

---

### **I. PURPOSE AND APPLICABILITY**

The purpose of this policy is to ensure that \_\_\_\_\_ implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain E-PHI into and out of \_\_\_\_\_, and the movement of this items within \_\_\_\_\_.

### **II. DETAILED POLICY STATEMENT**

1. The SO must develop and implement policies and procedures regarding media re-use. Specifically, the policy/procedure must address the removal of E-PHI from electronic media before the media can be made available for re-use. Please consult \_\_\_\_\_'S HIPAA Disposal Policy for information regarding appropriate techniques to utilize in order to assure that media systems used to store E-PHI can be appropriately re-used.
2. The SO must ensure that \_\_\_\_\_ remains accountable for E-PHI. This means that the SO must develop procedures to maintain and record the movements of hardware and electronic media. In addition, the SO should document the person responsible for keeping track of specific pieces of hardware/electronic media.
3. The SO must develop and implement a policy/procedure pertaining to data backup and storage. The policy/procedure must provide for a way to retrieve an exact copy of E-PHI, when needed, before the movement of any equipment can transpire.

### **III. RESPONSIBILITY**

1. All Workforce Members, Business Associates, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. The SO is responsible for implementing and maintaining this Policy.

### **IV. DOCUMENTATION**

1. The documentation called for under this Policy must be retained for a period of six (6) years from the date created or last in effect, whichever is longer.

### **V. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_, or the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.

## HIPAA PHI De-Identification Policy

---

### I. PURPOSE AND APPLICABILITY

The purpose of this Policy is clearly layout the procedures that must be followed when de-identifying PHI. The Privacy Rule only prevents \_\_\_\_\_ from disclosing patient information that is personally identifiable. Accordingly, \_\_\_\_\_ may use or disclose health information that is de-identified without restriction under HIPAA. Under §164.514(a) health information has been properly de-identified as long as the information is not individually identifiable and the \_\_\_\_\_ has no reasonable basis to believe that the information could be used to identify the individual. HIPAA allows for PHI to be de-identified in only one of two ways. The first is the expert determination method and the second is the safe harbor method.

All Workforce Members, Business Associates, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.

### II. DETAILED POLICY STATEMENT

#### Expert determination method

1. A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
  - i. Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
  - ii. Documents the methods and results of the analysis that justify such determination.
2. Whether a Workforce Member or Business Associate has sufficient knowledge and skill to be deemed an expert is a matter of professional judgement; OCR does not list a specific set of criteria that must be met. Consequently, the Privacy Officer is charged with determining whether a Workforce member has the requisite qualifications to de-identify PHI under the expert determination method. A Business Associate may serve as an expert only when \_\_\_\_\_ authorizes it to de-identify PHI on its behalf and in accord with the terms of the Business Associate agreement. The Business Associate must also comply with the procedures in this Policy.

#### The safe harbor method

1. \_\_\_\_\_ can properly de-identify PHI by scrubbing the following 18 identifiers of the individual or of relatives, employers, or household members of the individual, and it must not have actual knowledge that the scrubbed information could

be used alone or in combination with other information to identify an individual who is a subject of the information:

- Names.
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
  1. The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.
  2. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
- Telephone numbers.
- Facsimile numbers.
- Electronic mail addresses.
- Social security numbers.
- Medical record numbers.
- Health plan beneficiary numbers.
- Account numbers.
- Certificate/license numbers.
- Vehicle identifiers and serial numbers, including license plate numbers.
- Device identifiers and serial numbers.
- Web universal resource locators (URLs).
- Internet protocol (IP) address numbers.
- Biometric identifiers, including fingerprints and voiceprints.
- Full-face photographic images and any comparable images.
- Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification.

2. Any Workforce Member may de-identify PHI under the safe harbor method provided it is a requirement of their job duties and they have been directed to do so by the Privacy Officer. A Business Associate may de-identify PHI on behalf of \_\_\_\_\_ only if authorized to do so under the Business Associate agreement. The Business Associate must also comply with the procedures in this Policy.

### **Re-identification**

1. \_\_\_\_\_ may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by \_\_\_\_\_ provided that: The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and \_\_\_\_\_ does not use or

disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

2. Only those Workforce Members who have been instructed by the Privacy Officer or his/her designee should engage in re-identification activities.
3. Business Associates may engage in re-identification activities only if authorized to do so under the Business Associate agreement. The Business Associate must also comply with the procedures in this Policy.

### **III. RESPONSIBILITY**

1. All Workforce Members, Business Associates, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. The Compliance Officer and the Security Officer should work together to ensure that all forms of PHI are appropriately de-identified.

### **IV. DOCUMENTATION**

1. The person certifying statistical de-identification, under the expert determination method described in this Policy, must document the methods used as well as the result of the analysis that justifies the determination. \_\_\_\_\_, as a covered entity, is required to keep such certification, in written or electronic format, for at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.

### **V. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_, or the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.

## HIPAA Evaluation Policy

---

### I. PURPOSE AND APPLICABILITY

The purpose of this Policy is to ensure that \_\_\_\_\_ has a procedure in place to evaluate all of the policies and procedures that it is required to create under the Security Rule.

All Workforce Members, Business Associates, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy §164.308(a)(8).

### II. DETAILED POLICY STATEMENT

1. §164.308(a)(8) requires \_\_\_\_\_ to perform periodic technical and nontechnical evaluation, based initially upon the standards implemented under the Security Rule and, subsequently, in response to environmental or operational changes affecting the security of E-PHI, that establishes the extent to which a covered \_\_\_\_\_'s security policies and procedures comply with Subpart C of Part 164 of HIPAA.
2. Notwithstanding anything to the contrary, \_\_\_\_\_ will review its policies and procedures pertaining to the Security Rule on at least a quarterly basis.
3. The SO will be responsible for evaluating the effectiveness of \_\_\_\_\_'S policies and procedures.
4. The SO must be sure to document the evaluation, its results, and any proposed policy changes that should be implemented as a result of the evaluation.

### III. RESPONSIBILITY

1. All Workforce Members, Business Associates, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. The Compliance Officer and the Security Officer should work together to ensure that all forms of PHI are disposed of properly.

### IV. DOCUMENTATION

Any documentation required under this Policy must be retained for 6 years from the date of its creation or the date in which it was last modified, whichever is longer.

### V. GETTING HELP

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_, or the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.



## **HIPAA PHI Document Retention Policy**

---

### **I. PURPOSE AND APPLICABILITY**

The purpose of this Policy is to clarify the types of documents that must be retained as required under §164.316(b)(1) and (2). In relevant part, said section asserts that \_\_\_\_\_ must retain documentation of the policies and procedures implemented to comply with HIPAA and records of any action, activity, or assessment.

### **II. DETAILED POLICY STATEMENT**

1. HIPAA does not have a requirement for the retention of medical records. The retention of medical records is determined by state law, and to the extent applicable, Medicare. Accordingly, if \_\_\_\_\_ has questions regarding the retention requirements for medical records then it should consult its state specific statutes and CMS.
2. While HIPAA does not regulate the retention of medical records, it does regulate and call for, the retention of HIPAA related documents. Specifically, HIPAA asserts that \_\_\_\_\_ (covered entity) must retain documentation of the policies and procedures implemented to comply with HIPAA and records of any action, activity, or assessment.
3. The documentation must appear in written form (which may be electronic). §164.316(b)(2)(i) makes clear that any required documentation must be retained for a period of 6 years from the date of its creation or the date when it was last in effect, whichever is later.
4. The following is a list of document types that are subject to retention under HIPAA:
  - Accounting of disclosures of protected health information (PHI)
  - Authorizations for the disclosure of PHI
  - Breach notification & incident documentation
  - Business Associate agreements
  - Complaint & resolution documentation
  - Contingency & disaster recovery plans
  - Data use agreements and other forms supporting HIPAA compliance
  - Employee sanction policies
  - Information security & privacy policies
  - IT security system reviews
  - Log reports pertaining to the access of PHI
  - Notice of Privacy Practices
  - Records pertaining to the maintenance and updating of administrative, physical, and technical safeguards
  - Risk assessments and risk analyses security and privacy policies and procedures implemented to comply with HIPAA.
5. \_\_\_\_\_ must make the documentation available to those Workforce Members responsible for implementing the procedures to which the documentation pertains.

6. \_\_\_\_\_ must review required documentation periodically, and update as needed, in response to environmental and operational changes affecting the security of PHI.

### **III. RESPONSIBILITY**

1. All Workforce Members, Business Associates, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. The Compliance Officer shall be responsible for ensuring the implementation of this Policy.

### **IV. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_, or the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.

## Complaint Investigations & Compliance Review Policy

### I. PURPOSE AND APPLICABILITY

The purpose of this Policy is to ensure that \_\_\_\_\_ has the proper procedures in place to comply with complaint investigations and compliance reviews conducted by HHS.

### II. DETAILED POLICY STATEMENT

1. \_\_\_\_\_ must provide a process for individuals to make complaints concerning \_\_\_\_\_'S policies and procedures that are required by the Privacy Rule and Breach Notification Rule, or its compliance with such policies and procedures or the Privacy Rule and Breach Notification Rules.
  - Inform persons of their right to file a complaint. \_\_\_\_\_ will inform persons that they may complain to \_\_\_\_\_ and/or to the Secretary of the U.S. Department of Health and Human Services if they believe their privacy rights have been violated.
  - Filing a complaint. \_\_\_\_\_ may provide the following assistance when a person wishes to file a complaint:
  - Complaints to \_\_\_\_\_. If a person (including, but not limited to, a client, employee, Business Associate, independent contractor, accrediting organization, advocacy agency, or other person, association, group, or organization) wishes to complain to \_\_\_\_\_, the person may contact or may be directed to the Contact Person. The Contact Person, or his or her designee, may ask the person whether he or she wishes to submit a written or oral complaint. The complaint should be made in sufficient terms to enable the Contact Person to investigate, review, and resolve the complaint.
    - Written complaints. If the person wishes to submit a written complaint, the person may complete \_\_\_\_\_'s complaint form, or in a letter state in clear terms the nature of the complaint, and/or provide any other information necessary to enable \_\_\_\_\_ to investigate, review, and resolve the complaint. The Contact Person, or his or her designee, shall ensure that the person has filled out the complaint form completely and has provided sufficient information to enable the respective organization to investigate, review, and resolve the complaint.
    - Oral Complaints. The Contact Person, or his or her designee, may document the oral complaint in writing.
  - Complaints to HHS. If a person wishes to complain to the Secretary, the person shall be provided with information sufficient to make a written complaint, either in paper or electronic form. The complaint must name the respective organization and describe the acts or omissions believed to be in violation of the Privacy Standards or Security Standards. It shall be filed within one-hundred and eighty (180) days of when the person knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown. More information on filing a complaint with HHS can found on

HHS's website. Visit <https://www.hhs.gov/hipaa/filing-a-complaint/complaint-process/index.html>

- Report to \_\_\_\_\_ Management. The Contact Person shall forward all written and oral privacy complaints to the applicable \_\_\_\_\_ Management.
2. \_\_\_\_\_ must refrain from retaliating against, or intimidating, any individual for exercising their right to raise a complaint.
  3. \_\_\_\_\_ may not require an individual to waive any right granted under §160.306, the Privacy Rule or the Breach Notification Rule, as a condition of the provision of treatment, payment, or enrollment in a health plan or eligibility for benefits.
  4. \_\_\_\_\_ must keep records and submit compliance reports (in the time, manner, and containing the information) as HHS deems necessary for it to evaluate the \_\_\_\_\_'S compliance with the administrative simplification provisions (45 C.F.R. § 160.310(a)).
  5. \_\_\_\_\_ must cooperate with HHS if it begins an investigation or compliance review of \_\_\_\_\_'S policies or practices to determine whether \_\_\_\_\_ is complying with the HIPAA administrative simplification provisions (45 C.F.R. § 160.310(b)).
  6. \_\_\_\_\_ must allow HHS access, during normal business hours, to their:
    - Facilities, books, and records.
    - Accounts and other information, including protected health information (PHI).(45 C.F.R. § 160.310(c).)

If HHS determines that "exigent circumstances" exist (for example, the possibility that documents may be hidden or destroyed), it may request access from \_\_\_\_\_ without notice, at any time. In some cases, information that a \_\_\_\_\_ must allow HHS to access may be in the exclusive possession of another agency, institution, or person. If the other agency, institution, or person fails or refuses to provide the information to \_\_\_\_\_, then it must:

- Certify this fact.
- Describe what efforts it has made to obtain the information.

PHI obtained by HHS in connection with an investigation or compliance review under the rules requiring HHS access will not be disclosed by HHS, unless:

- Necessary for determining or enforcing compliance with the HIPAA Rules.
- Otherwise required by law.

- Permitted under 5 U.S.C. Section 552a(b)(7), which allows disclosure of records in certain situations in response to a written request from another US agency (for example, a state attorney general for civil or criminal law enforcement).

### **III. RESPONSIBILITY**

1. All Workforce Members, Business Associates, and anyone else who handles PHI on behalf of \_\_\_\_\_ is responsible for complying with this Policy.
2. The Compliance Officer shall be responsible for ensuring the implementation of this Policy.

### **IV. DOCUMENTATION**

The documentation required by this Policy must appear in written form (which may be electronic) and be retained for a period of 6 years from the date of its creation or the date when it was last in effect, whichever is later.

### **V. GETTING HELP**

For questions about this policy, or to escalate an issue, please contact the Privacy Officer at \_\_\_\_\_ or \_\_\_\_\_, or the Security Officer at \_\_\_\_\_ or \_\_\_\_\_.

## Civil Money Penalties Overview

On April 30, 2019, HHS changed its interpretation of cumulative annual civil money penalty limits for HIPAA violations. The new penalties interpretation is “effective indefinitely”.

This change in interpretation results in the following, updated HIPAA penalty structure:

	Culpability	Minimum Penalty/Violation	Maximum Penalty/Violation	Annual Limit
Tier 1	No knowledge	\$100	\$50,000	<b>\$25,000</b>
Tier 2	Reasonable cause	\$1,000	\$50,000	<b>\$100,000</b>
Tier 3	Willful neglect; corrected	\$10,000	\$50,000	<b>\$250,000</b>
Tier 4	Willful neglect; not corrected	\$50,000	\$50,000	<b>\$1,500,000</b>

### Practical Impact

HHS' new interpretation means that the annual limit that \_\_\_\_\_ can be fined within a given year for Tier 1, 2, and 3 level violations has been reduced from \$1,500,000 to \$25,000, \$100,000, and \$250,000 respectively.