Reviewed:11/18/2022

HIPAA PRIVACY POLICY & PROCEDURE MANUAL

Company Name: Will be referred to as [Organization] throughout each policy.	**Advanced Metrics**
Policy Name:	Privacy Policy
Policy Version:	Version 2.0
Effective Date:	**11/18/2022**
Review Date:	Yearly
***Privacy Officer*: Will be referred to as *Privacy Officer* throughout each policy.**	**Martha Shetrompf**
Security Officer: Will be referred to as Security Officer throughout each policy.	**John Kreiner**
Compliance Officer: Will be referred to as Compliance Officer throughout each policy.	**Steven Herr**
Responsible for Review:	**Martha Shetrompf**

Table of Contents

HIPAA Confidentiality Agreement

As a *Workforce member* of **Organization**, I understand that **Organization**, a *covered entity* under the *HIPAA* regulations, has a legal responsibility to protect the privacy and security of patient Protected Health Information (*PHI*) and Electronic Protected Health Information (*ePHI).*

During the course of my employment with **Organization**, I may create, see, hear, or touch Protected Health Information (*PHI*), Electronic Protected Health Information (*ePHI*), and other information that **Organization** must maintain as confidential.

By reading and understanding this Confidentiality Agreement, I acknowledge and understand that:
PHI

- I will not use or disclose *PHI* or *ePHI*, except when necessary to perform my job.
- With respect to other types of confidential information, I will only *access*, use, or disclose such information if it is required for the performance of my job.
- I will keep all security codes and passwords used to *access* the facility, equipment or computer systems, confidential at all times.
- When my employment with the **Organization** is terminated or completed, I will immediately return all property to the **Organization**. This property includes, but is not limited to, keys, *access* cards, **Organization** documents however stored or maintained, and ID badges.
- Even after my employment is concluded, I agree to meet the use, disclosure, and confidentiality obligations under this Confidentiality Agreement.

By reading and understanding this Confidentiality Agreement, I am confirming that I am bound by its terms, and that I will perform my duties in accordance with those terms. I understand that if I violate or fail to follow the terms of this Confidentiality Agreement, I am subject to disciplinary action, including (but not limited to) termination of my employment and may be subject to civil or criminal penalties.

Introduction to the HIPAA Privacy Manual

HIPAA requirements generally cover the protection of and *access* to an *individual*'s health information and related financial and demographic information (name, date of birth, address) used to identify them and pay for health care. What most people refer to as *HIPAA* is really a group of several federal laws and many regulations enacted and revised over the course of the last 25 years.

It is the intent of this Policy Manual, along with our other Policy manuals and stand-alone policies, to reflect the Organization's responsibilities in ensuring a) the privacy, integrity and security of the information we use, transmit, create and maintain and b) the *individual's* rights for accessing, sharing, amending and accounting for use and disclosure of their PHI and to be notified when the PHI is shared or accessed when it should not have been. Your understanding of the protections to PHI's security and integrity, when and how *individuals* and others can access this information, and what to do when you notice it may have been used improperly are integral to your responsibility when working with this protected health information (PHI) on the Organization's behalf.

The Organization places safeguards to the privacy, integrity and security of PHI and you are responsible for following them. You are responsible for not using or sharing PHI when it is not required for you to perform your responsibilities. You are responsible for reading and understanding the Synopsis of all the Policies included here as well as the full content of any that apply directly to your role. The Organization requires that you read, understand, agree to abide by and attest to them. The Organization appreciates your efforts and contributions in meeting the requirements that apply to *individuals'* protected health information that has been entrusted to us.

The Policies in this Manual have been organized in a way to help you understand the general rules concerning sharing and protecting *PHI*, assuring an *individual*'s rights are met with regard to their own *PHI*, determining when requirements for authorizations apply, determining when an *individual* has the right to agree or object to the use or disclosure of their *PHI*, determining when no requirements for an opportunity to agree or object or an authorization are needed for the sharing of information, and special more complex rules around sharing *PHI* in certain instances like those involving minor's, deceased *individual*s, legal processes like subpoenas, law enforcement requests, emergency situations and judicial orders. Additionally, the Manual covers your responsibilities and requirements for identifying and reporting incidences of potential improper use or disclosure of *PHI* and the **Organization's** responsibilities for assessing incidents and giving appropriate notice for incidents that are determined to be a *breach* of the Privacy Rule. The table of contents, synopses or any search feature on your browser should help you in finding information to address most situations regarding the privacy of *PHI* you may encounter. Always contact the *Privacy Officer* or your supervisor for assistance when you are unsure how to proceed.

Privacy Manual Synopsis

This section is for all *Workforce members* to review and attest. Below is a summary of each policy, including the relevant *HIPAA* regulations. Please view the full content of any Policy that is directly applicable to your role and responsibilities in the Organization. To view the full policy, please click on the title of that section in the synopsis.

Definitions for the terms used in this manual are included in the Glossary at the end of the manual and defined terms are *italicized.*

Privacy Policy 1.0 HIPAA Privacy Program: General

Organization takes the privacy, security and integrity of *individuals*' protected health information very seriously**. Organization's** *Privacy Officer* oversees **Organization's** compliance with the *HIPAA* Privacy Rule. The *Privacy Officer* oversees **Organization's** efforts to secure and maintain the confidentiality and integrity of protected health information (*PHI*), maintain sensitive **Organization** information, prevent and detect inappropriate and illegal uses and disclosures of *PHI*, and assure *individuals'* rights with regard to accessing, *amend*ing and accounting for use and disclosure of their *PHI*. *Workforce members* must be familiar with the *Privacy Officer*'s job functions. *Workforce members* must be familiar with their responsibility to maintain the confidentiality and integrity of *PHI* and to disclose and use it only as allowed or required. *Workforce members* must contact the *Privacy Officer* when this Policy requires that they do so.

Organization will appoint a *Privacy Officer*, implement and operationalize policies and procedures, train its *workforce members*, safeguard protected health information, establish procedures for the receipt and response to complaints regarding *HIPAA* compliance, establish clear disciplinary process for violations of *HIPAA* requirements, mitigate any harm from improper use or disclosure of protected health information, prohibit retaliation against anyone seeking in good faith to enforce *HIPAA* rights or responsibilities, and appropriately retain *HIPAA* documentation. **Organization** may not require *individual*s to waive their rights to file a complaint with *HHS* regarding *HIPAA* compliance as a condition of the provision of *treatment*, *payment*, enrollment in a health plan, or eligibility for benefits.

45 CFR Part 164 Subpart E
45 CFR 164.530 HIPAA Privacy Program Administrative Requirements

Privacy Policy 2.0 Administrative, Technical and Physical Safeguards of PHI

Organization must safeguard and protect the privacy of *PHI* by instituting physical, administrative and technical safeguards. *Workforce members* must understand what

safeguards, are in place and abide by them to assure that *PHI* remains private and is only shared as is allowed under the Privacy Rule. Some examples of safeguards include locked doors, policies and procedures, training, complaint resolution, incident reporting and sanctions for violations of policies and procedures. *Workforce members* should refer to The Security Policy and Procedure Manual for specifics on **Organization's** safeguards for electronic *PHI* and equipment.

45 CFR 164.528(c): *Accounting of Disclosures of Protected Health Information: Safeguards*

Privacy Policy 3.0 Minimum Necessary Standard

Under the *minimum necessary standard*, **Organization** may generally only use, request, or disclose *PHI* that is necessary to fulfill a request, or perform a job function. *Workforce members* will be trained on this standard so that *PHI* is used, requested, or disclosed only to the extent that is legally required. You will also be instructed when the standard does not apply, for example, for purposes of *treatment*.

45 CFR 164.502(b)(1) *Minimum Necessary Standard*
45 CFR 164.514(d)(3) *Minimum Necessary Disclosures of Protected Health Information*
45 CFR 164.524(a) *Access to Protected Health Information*

Privacy Policy 4.0 Verification of Identity and Authority

Before **Organization** discloses *PHI* to an *individual* or another **Organization** requesting it, **Organization** must verify the identity of the *individual* or other organization and their authority where required. This policy outlines the requirements for identity and authority verification.

45 CFR 164.514(h)(1) *Standard Verification Requirements*

Privacy Policy 5.0 Complaints to the Organization

Organization must have a complaint process, under which *individual*s may make complaints about **Organization's** compliance with the *HIPAA* Privacy Rule, the *HIPAA Breach* Notification Rule, and **Organization's** policies and procedures related to these rules. **Organization** has designated the *Privacy Officer* as the person responsible for receiving these complaints. Any such complaints received by others, in whatever form, should be directed to the *Privacy Officer*'s attention as soon as possible. The *Privacy Officer*, in cooperation with whatever other resources they deem appropriate, will review complaints, document and respond to them. Any complaint that is received that is also a Privacy incident, will be handled according to the process set forth in Privacy Policy 6: *HIPAA Incident Response and Reporting and Breach Determination*. **Organization** will also act to prevent anyone from intimidating, threatening, coercing, discriminating against, or retaliating against any *individual* who has exercised their

right under *HIPAA* to file complaints with the **Organization** concerning it's *HIPAA* compliance.

45 CFR 164.530(a)(d) and (g)*Administrative Requirements: Personnel Designations, Complaints and Refraining from Intimidating or Retaliatory Acts*
45 CFR 164.524(d) *Individual Right: Right to file Complaint Concerning Denial of Access*
45 CFR 164.520(b)(1)(vi) *Notice of Privacy Practice: Complaints*

Privacy Policy 6.0 HIPAA Incident Response and Reporting and Breach Determination

Organization takes the privacy, security and integrity of *individuals'* data seriously. **Organization** also has legal responsibilities to protect *PHI* under *HIPAA*, to identify and respond to suspected incidents, mitigate harm, require its *workforce members* to report incidents, and to determine when there is a reportable *breach* of an *individual*'s *PHI*.

The purpose of this *Breach* Determination Policy is to meet **Organization's** responsibilities and to provide guidance to **Organization** *workforce members* on how to recognize and report a privacy or *security incident* involving Member health information. **Organization** will review all reported incidents and will follow the procedures set forth to determine if there has been a *Breach* (an acquisition, *access*, use, or disclosure of the Member's *unsecured PHI* in a manner not permitted under *HIPAA*).

This policy establishes guidelines for Organization to:

Require the reporting of suspected privacy and *security incident*s (any attempted or successful unpermitted or unauthorized *access*, use, disclosure, modification, interference or destruction of *unsecured PHI* in any form). All *workforce members* are required to report any suspected incident to the Compliance, Privacy or Security Officer as soon as possible, and may report anonymously through The Guard if preferred. Failure to promptly report any suspected or known incident will result in disciplinary action. Refer to Privacy Policy 8.0: *Sanctions/Discipline* for further details.

Identify and respond to suspected or known incidents involving the security or privacy of protected health information, including mitigating any harmful effects. Any complaint that is filed with the Organization that is potentially a privacy or *security incident* will be handled under this Policy, which also appears in the Security manual, instead of Privacy Policy 5.0: *Complaints to the Organization*.

Determine if there has been a *Breach* of *unsecured PHI* ("*PHI*") after analyzing potential exceptions and performing a risk analysis, and

Document the incidents, responses and *Breach* determinations.

Follow the *Breach* Notification Policy whenever it determines that a *Breach* has occurred. Privacy Policy 7: *Breach Notification*.

45 CFR 164.308(a)(6)(i) *Security Incident Procedures*
45 CFR 164.308(a)(6)(ii) *Implementation Specification: Response and Reporting (Required)*
45 CFR 164.530(a)(c)(e)(f) *Administrative Requirements: Personnel Designations, Safeguards, Sanctions and Documentation, Mitigation*
45 CFR 402 *Definitions: Breach*

Privacy Policy 7.0 Breach Notification

Organization takes the privacy and integrity of *individuals'* personal health information seriously. **Organization** also has legal responsibilities to protect *PHI* under *HIPAA*, to determine when there is a reportable *breach* of an *individual*'s *PHI* and to make appropriate and timely notifications following a *breach*.

The purpose of this *Breach* Notification Policy is to meet **Organization's** responsibilities and to provide guidance to **Organization** *workforce members* regarding making required notifications when a *Breach* determination has been made under Privacy Policy 6.0: *Incident Response and Reporting and Breach Determination*.

This *Breach* Notification Policy establishes guidelines for **Organization** to

- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to *individual*s impacted by a *Breach*,
- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to federal and state authorities if required by the details of the *Breach* determination,
- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to media if the findings of the *Breach* determination require them;
- Determine when and if appropriate substitute notice is allowed and to use that substitute notice when appropriate; and
- Document compliance with the requirements of *Breach* notifications.

45 CFR 164.404 *Notification to Individuals*
45 CFR 164.406 *Notification to the Media*
45 CFR 164.408 *Notification to the Secretary*
45 CFR 164.410 *Notification by a Business Associate*
45 CFR 164.412 *Law Enforcement Delay*
45 CFR 164.414 *Administrative Requirements and Burden of Proof*
45 CFR 164.530 *Administrative Requirements*

Privacy Policy 8.0 Sanctions/Discipline

Workforce members who violate **Organization's** privacy policy and procedures are subject to sanctions. Sanctions are disciplinary measures intended to address violations and to deter future violations. **Organization**, in deciding upon the appropriate sanction, may review the severity of the violation, the impact of the violation, and the *workforce member's* work history. Sanctions imposed will be consistent, and proportional with the severity of the offense. Discipline up to and including termination, even for first violations, may be appropriate.

45 CFR 164.530(e) *Sanctions*

Privacy Policy 9.0 Business Associates

Organization relies on *business associates*, which are vendors that handle *PHI* (create, receive, maintain or transmit) on behalf of or for the benefit of **Organization** to carry out **Organization's** *HIPAA* functions. This policy covers how **Organization's** *workforce* determines who is a *business associate*. The policy then covers the details and requirements of the *business associate* contract the **Organization** and a *business associate* must enter into to protect the privacy of health information, requirements for reporting incidents and *breach*es, what to do when those contracts end and the O**rganization's** due diligence to assure vendors properly handle *PHI* and train their *workforce members*.

45 CFR 160.103 *Business Associate Definition*
45 CFR 164.502(3)-(4) *Permitted and Required Uses and Disclosures; Business Associates*
45 CFR 164.504(e) *Standard Business Associate Contracts*

Privacy Policy 10.0 Notice of Privacy Practices

Organization must provide patients with its Notice of Privacy Practices unless an exception for group health plans or inmates applies. This notice describes how patient *PHI* is to be used and disclosed under the Notice of Privacy Practice. *Workforce members* should be familiar with where to find the Notice of Privacy Practices in electronic and paper form and should provide *access* to *individual*s on first contact with the **Organization** and upon request. *Workforce members* should be familiar with the contents of the Notice of Privacy Practices and follow it.

45 CFR 164.520 *Notice of Privacy Practices for protected health information*

Privacy Policy 11.0 Use and Disclosure of PHI: General Rules

In general, *covered entities* and *business associates* may not use or disclose protected health information, except when the Privacy Rule specifically permits or requires such use or disclosure. This policy and the ones immediately following it inform the *workforce* on when the Privacy Rule permits and requires use or disclosure of protected health information, documentation related to different required or permitted uses and disclosures and other

details related to each circumstance. If a *workforce member* is unsure whether to allow or deny a use or disclosure that is related to their job responsibilities, they should reach out to their supervisor or the *Privacy Officer* for clarification before acting.

45 CFR 164.502 *Uses and Disclosures of Protected Health Information: General Rules*
45 CFR 164.501 *Definitions*
45 CFR 160.203 *General Rule and exceptions*

Privacy Policy 12.0 Uses and Disclosures: *Individual* Opportunity to Agree or Object Required

Under some circumstances, **Organization** must provide an *individual* the opportunity to agree or object to disclosure of *PHI*.
Organization will afford *individual*s the opportunity to agree or object to a use or disclosure in the following circumstances:

1. disclosure of *PHI* to a person that is directly relevant to that person's involvement with an *individual*'s care including *payment* for that care,
2. limited disclosure for notification of an *individual*'s location, general condition or death,
3. uses and disclosures for disaster relief purposes and
4. uses and disclosures when an *individual* is deceased (prior prohibition on disclosures must be honored) and
5. use and disclosure of *PHI* by the **Organization** for purposes of a *facility directory* if the **Organization** is currently using one,

This policy covers how **Organization** provides such an opportunity and honors an *individual*'s choices. *Workforce members* will only use or disclosure information in the above listed circumstances as described in this policy. *Workforce members* will afford *individual*s an opportunity to agree or object to such uses and will reflect any oral agreements or objections in the *individual*'s record. Other requirements may override an *individual*'s right, for example a response to a judicial or administrative order. If a *workforce member* is not sure how to proceed, they should consult their supervisor or the *Privacy Officer* before using or disclosing information in the above circumstances.

45 CFR 164.510 *Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object*

Privacy Policy 13.0 Uses and Disclosures: Authorization Required and Requirements for a Valid Authorization

Organization will obtain and require valid written *individual* authorization before it uses or discloses information in the circumstances described in this policy and as required under the

Privacy Rule. Generally, **Organization** may not use or disclose *PHI* without a valid written authorization from the *individual* who is the subject of the information, unless otherwise allowed under the Privacy Rule. When the *individual* provides a valid authorization, **Organization's** use and disclosure of the information must be consistent with the authorization. *Workforce members* must be familiar with the requirements of a valid authorization and the situations which require that authorization be obtained prior to use or disclosure of information and must follow the terms of the authorizations that are in place. See Privacy Policy 14: *Use and Disclosure: No Authorization or Right to Agree or Object* for more detail on situations in which an authorization is not required.

Organization allows revocation of authorizations in writing with some minor exceptions as further detailed below. **Organization** will provide *individual*s with a copy of their authorizations. **Organization** will use and accept only valid authorization forms written in plain language which contain all the core elements and required statements for an authorization and will limit the use of compound authorizations to circumstances where they are allowed as detailed in the full policy. The **Organization** will also document and retain any signed authorization.

Organization will not condition the provision of *treatment*, *payment*, enrollment in a health plan, or eligibility for benefits on the provision of an *individual*'s authorization except in limited circumstances as allowed under the Privacy Rule and further described in the policy. **Organization** will meet the requirements for authorizations related to the sale of *PHI* and communications for marketing purposes.

45 CFR 164.508 *Uses and Disclosures for Which an Authorization is Required*
45 CFR 501 *Definitions*

Privacy Policy 14.0 Uses and Disclosures: No Authorization or Opportunity to Agree or Object Required

Under certain circumstances, **Organization** may use and disclose *PHI* when neither authorization nor an opportunity for an *individual* to agree or object is required. This policy informs ***Workforce members*** of what those circumstances are, and what steps ***Workforce members*** must take to fulfill requests for *PHI* when no authorization or opportunity for an *individual* to agree or object is required. Generally, written authorization or an opportunity to agree or object are not required when a use or disclosure is for *treatment*, *payment*, or healthcare operations purposes. In addition, written authorization or an opportunity to agree or object are generally not needed when a law *requires* that **Organization** use or disclose certain *PHI*. There are a few additional special circumstances that allow disclosure like for use by a *whistleblower*, the victim of a crime while at work at the **Organization**, and for Military and Veteran Activities.

Each *workforce member* should be familiar with what activities are included in *treatment*, *payment* and *health care operations* under the Privacy Rule. Frequently referred to as TPO, it is very important for work force *members* to understand the scope of what is covered because it informs many of the day-to-day privacy and information *access* decisions they will be making concerning the use and disclosure of *PHI*. If a *workforce member* is unsure of what is included, they should review this policy and seek assistance from their supervisor or the *Privacy Officer* for clarity.

45 CFR 164.501 *Definitions: Healthcare Operations*
45 CFR 164.512 *Uses and Disclosures for which an Authorization or Opportunity to Agree or Object is Not Required*
45 CFR 164.506 *Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations*

Privacy Policy 15.0 Individual Right: Access to Protected Health Information

Organization must afford *individual*s the opportunity to *access* and inspect their protected health information maintained in a *designated record set*. This policy covers how work force *members* must timely respond to requests for *access*, inspection, and copies of *medical record*s by *individual*s and their *personal representative*s; when such requests can or must be denied; if and how an *individual* can appeal a denial of *access*; in what format the *individual* may request and receive the records; and what fees may be charged for fulfilling the requests.

45 CFR 164.524 *Access of Individuals to Protected Health Information*

Privacy Policy 16.0 Individual Right: Request Restrictions and Alternate Confidential Communications

When feasible or required, **Organization** will honor *individuals'* requests to restrict uses and disclosures of *PHI* that are made to carry out *treatment*, *payment*, or *health care operations*, and that are made to family, friends, or others for involvement in care and notification purposes. **Organization** will also honor requests made by *individual*s to receive communications of *PHI* by alternative means or at an alternate location when feasible or required. *Workforce members* shall be trained as to how to respond to all such requests. All such requests shall be required to be in writing or reflected in the record in writing at the time of the request. *Workforce members* need to be aware how to reflect and find these requests in the *individual*'s records.

45 CFR 164.502(c) *Uses and Disclosures of PHI Subject to an Agreed Upon Restriction*
45 CFR 164.502(h) *Confidential Communications*
45 CFR 164.522 *Rights to Request Privacy Protection for Protected Health Information*

Privacy Policy 17.0 Individual Right: Request Amendment of Designated Record Set

*Individual*s have the right to request *amendment* to certain protected health information in the *designated record set* of their *medical record*s. *Amendment* can consist of adding *PHI* to an existing record, or supplementing a record by, for example, submitting a second opinion. **Organization** and its *workforce* shall promptly respond to requests to *amend PHI*, and promptly inform *individual*s as to whether their request is granted or denied. Contact your *Privacy Officer* if you receive a request for an *amendment* to *PHI* or notification from another *Covered entity* of an *amendment* to *PHI* in **Organization's** records.

45 CFR 164.528 *Accounting of Disclosures of Protected Health Information*

Privacy Policy 18.0 Individual Right: Accounting of Disclosures

*Individual*s have the right to receive an ***accounting of disclosures*** of their protected health information ("*PHI*") that have been made by **Organization** to another entity, including disclosures to or by *business associates*. Several categories of uses and disclosures are excluded from accountings such as those requested by the *individual* themselves or those made to other entities and persons for *treatment* purposes. *Individual*s can exercise this right to an accounting by making a written request to **Organization**. **Organization** must properly respond to the request and send the accounting when appropriate. **Organization** will handle requests for accountings of disclosures through the *Privacy Officer* or their designee.

45 CFR 164.528 *Accounting of Disclosures of Protected Health Information*

Privacy Policy 19.0 Uses and Disclosures: Psychotherapy notes

Psychotherapy notes are treated differently from other mental health information both because they contain particularly sensitive information and because they are the personal notes of the therapist that typically are not required or useful for *treatment*, *payment*, or *health care operations* purposes, other than by the mental health professional who created the notes. This policy describes how **Organization** is to respond to requests for *psychotherapy notes*; the distinction between *psychotherapy notes* and other mental health records; the mental health practitioner/patient privilege that applies to *psychotherapy notes*; and the requirement that these notes be separated from the *designated record set* to receive heightened protections. The Policy also describes the processes **Organization** will follow to assure that it meets all requirements for use and disclosure of *psychotherapy notes* in the limited circumstances where it is allowed.

This policy serves to train **Organization** *workforce members* as to what constitutes *psychotherapy notes*, and when such notes may be used or disclosed.

45 CFR 164.508(a)(2) *Uses and Disclosures for Which an Authorization is Required: Psychotherapy notes*

Privacy Policy 20.0 Minors' Rights

This policy covers when minors must *access* their *PHI* through a *personal representative*, and when minors may *access* their *PHI* directly. **Organization** *workforce members* must be familiar with the circumstances under which minors can *access* their *PHI* without parental, guardian or *personal representative* approval or knowledge. **Organization** *workforce members* should also be familiar with the circumstances where parents, guardians and *personal representative*s of minors cannot *access* a minor's record without the minor's approval.

45 CFR 164.502(g) *Personal Representatives, Adults and Emancipated Minors*

Privacy Policy 21.0 Use of Social Media

This policy outlines the safeguards *Workforce members* must follow to ensure that their use of social media does not result in unauthorized disclosure of *PHI*. It applies to both professional and personal accounts and social media platforms. *Workforce members* using social media must take precautions to ensure *PHI* is not accidentally or intentionally disclosed during such use. This policy describes what precautions must be taken.

45 CFR 164.530(c) *Privacy Safeguards*

Privacy Policy 22.0 Uses and Disclosures: Response to Judicial and Administrative Proceedings

Organization must disclose a patient's *PHI* when that *PHI* is properly sought in a judicial or administrative proceeding. Such proceedings include civil and criminal court proceedings, and proceedings before government agencies, such as Professional Licensing Boards, the Department of Health and Human Services ("*HHS*") and the Centers for Medicare and Medicaid Services ("CMS"). **Organization** will respond to judicial or administrative orders, as well as subpoenas, discovery requests, or other lawful process, that is not accompanied by an order of a court or *administrative tribunal*, if certain criteria are met, including the provision of satisfactory assurances. ***Workforce members*** will be trained as to how to respond to requests for *PHI* sought in these proceedings and should always contact the Compliance or *Privacy Officer* if they receive a request directly.

45 CFR164.512(e) *Use and Disclosure of Protected Health Information for Judicial and Administrative Proceedings*

Privacy Policy 23.0 Uses and Disclosures: Fundraising

Organization may use and disclose an *individual's PHI* for certain *fundraising* purposes for its own benefit subject to certain restrictions, including the need for an authorization in some circumstances. **Organization** must permit *individual*s the right to opt out of receiving *fundraising* communications, and to not receive the communications after opting out. **Organization** will not share an *individual*'s information for *fundraising* purposes unless its Notice of Privacy Practice contains provisions regarding the **Organization's** potential *fundraising* activity, the right to opt out, stop receiving fund raising communications, and to change their mind and ask to receive them again.

45 CFR 164.514(f)(2) *Uses and Disclosures for Fundraising & Implementation Specifications: Fundraising Requirements*
45 CFR 164.501 *Definitions*

Privacy Policy 24.0 Uses and Disclosures: Worker's Compensation

This policy provides rules for **Organization's** use or disclosure of *PHI* for worker's compensation, or other similar programs established by law, that provide benefits for work-related injuries or illness without regard to fault. **Organization** follow's *HHS* guidance for complying with these varied laws in a number of ways including allowing disclosures without an *individual*'s authorization, allowing disclosures with an *individual*'s authorization, and requiring the application of the *minimum necessary standard* for worker's compensation disclosures. This policy describes the circumstances under which such disclosure is required, is allowed and how to make the disclosure.

45 CFR 164.512(l) *Uses and Disclosures for which an Authorization or Opportunity to Agree or Object is Not Required: Worker's Compensation*

Privacy Policy 25.0 Limited Data Set and Data Use Agreements

Organization may share a **Limited Data Set**, which is a set of *PHI* with certain identifiers removed, to a requesting party who seeks the *PHI* disclosure for purposes of *research*, public health, or healthcare operations. Such disclosure may only be made if the **Organization** obtains a signed, written Data Use Agreement (DUA) from the person or entity to whom the **Limited Data Set** is to be disclosed. This policy defines a *limited data set*; sets forth appropriate uses for *limited data set*s; requires that a data use agreement meeting the defined criteria be in place

between the parties; requires that the **Organization** adhere to applicable data use agreements and monitor the recipient's use of the data set for patterns of activity or practices in violation of the data use agreement, and requires **Organization** to end sharing of the data set and report to *HHS* if any violations are not reasonably cured

45 CFR 164.514(e) *Limited Data Set and Data Use Agreement*

Attestation

I hereby attest and acknowledge that I have read and understood the contents of this *HIPAA* Privacy Policy and Procedure Manual. Through my attestation, I hereby confirm that I am bound by **Organization's** privacy policies and procedures and will perform my job duties accordingly. I understand that if I violate any **Organization** privacy policy or procedure, I am subject to disciplinary action, up to and including termination of my employment. I may also be subject to civil or criminal penalties.

I hereby acknowledge and agree that this attestation is the equivalent of a physical or e-signature.

Privacy Policy 1.0 HIPAA Privacy Program: General

FULL POLICY LANGUAGE:

Policy Purpose:

Organization will comply with its responsibilities to ensure the privacy, integrity and security of the information we use, transmit, create and maintain as well as the *individual* 's rights for accessing, sharing, *amend*ing and accounting for use and disclosure of their *PHI* and to be notified when the *PHI* is shared or accessed when it should not have been.

Policy Description:

Organization will appoint a *Privacy Officer*, implement and operationalize policies and procedures, train its *workforce members*, safeguard protected health information, establish procedures for the receipt and response to complaints regarding *HIPAA* compliance, establish clear disciplinary process for violations of *HIPAA* requirements, mitigate any harm from improper use or disclosure of protected health information, prohibit retaliation against anyone seeking in good faith to enforce *HIPAA* rights or responsibilities, and appropriately retain *HIPAA* documentation. **Organization** may not require *individual*s to waive their rights to file a complaint with *HHS* regarding *HIPAA* compliance as a condition of the provision of *treatment*, *payment*, enrollment in a health plan, or eligibility for benefits.

At all times, **Organization** shall have one individual identified and assigned to *HIPAA* Privacy responsibility. This individual is known as the *HIPAA Privacy Officer*. **Organization's** *workforce members* must understand the protections to *PHI*'s security and integrity, when and how *individual*s and others can *access* this information, and what to do when they notice it may have been used improperly when working with this protected health information (*PHI*) on the **Organization**'**s** behalf.

The *Privacy Officer* is responsible for **Organization's** overall compliance with the *HIPAA* Privacy Rule, and for ensuring that **Organization's** *HIPAA* Privacy Rule policies and procedures are developed, implemented, and followed. The *Privacy Officer* is the point person for **Organization's** Privacy Program, through which the *Privacy Officer*'s and other **Organizational** duties are carried out.

The **Organization** must follow the below procedures under the Privacy Program.

Procedures:

Designation of Individuals:

1. Designation of the *Privacy Officer*, who is responsible for development and implementation of **Organization's** policies and procedures.
2. Designation of a contact person or an office (may be either the *Privacy Officer* or another designated individual or location) responsible for receiving privacy-related complaints, and provide further information about **Organization's** Notice of Privacy Practices.

Training:

1. **Organization** must train all *workforce members* on its Privacy Policies and Procedures, as necessary and appropriate for *workforce members* to carry out their functions within the **Organization**. Training shall be provided as follows:
    a. To each new *member* of the *workforce* within a reasonable period of time after the person joins the *workforce*;
    b. To each *member* of **Organization's** *workforce* whose functions are affected by a significant change in **Organization's** privacy policies and procedures, within a reasonable period of time after that change becomes effective.
    c. To any *member* of the *workforce* whose responsibilities have changed when different policies and procedures apply to their new role.
    d. **Organization** must document that the training has been provided.
2. Questions concerning training or any aspect of training may be directed to the *Privacy Officer*.

Safeguards:
Organization must reasonably safeguard protected health information (*PHI*) from any intentional or unintentional use or disclosure that violates the *HIPAA* Privacy Rule. **Organization** must also reasonably safeguard protected health information to limit incidental *PHI* uses or disclosures that are made pursuant to an otherwise permitted or required use or disclosure. Following a risk assessment of the *PHI* held by Organization, it shall implement Physical, Administrative and Technical safeguards to reasonably address the risk of improper *access*, use or disclosure of *PHI* in all forms including oral, visual, paper, electronic (addressed separately in the security policy), film, or any other format.
Examples of appropriate safeguards by type are:
Administrative safeguards – Policies and Procedures including discipline, training, and guidance, sign in sheets;
Physical Safeguards: locks, segregation of *PHI* in secured areas, *access* restrictions;
Technical Safeguards: encryption, key card *access*, firewalls, *access* reviews.

Organization will conduct physical audits of its locations to identify and address risks which require reasonable safeguards to be implemented. **Organization** will review privacy complaints and incidents on an annual basis, or more frequently if a significant number of complaints are received or incidents occur, to determine if additional safeguards are necessary for any recurring incident or complaint types.

Complaints:
Organization must provide a process for *individual*s to make complaints concerning its compliance with the *HIPAA* Privacy Rule, the *HIPAA Breach* Notification Rule, and **Organization's** policies and procedures related to these rules. **Organization** will address all complaints received and keep records of complaints and their resolution. Please refer to Privacy Policy 5.0: *Complaints to the Organization* for more details. **Organization** will handle

any complaints that are also found to be Privacy incidents under Privacy Policy 6.0; *HIPAA Incident Response and Reporting and Breach Determination*.

Sanctions:
Organization must develop and apply appropriate sanctions against *workforce members* who fail to comply with its privacy policies and procedures and/or the *HIPAA* Privacy Rule. **Organization** must document all sanctions and apply them in a consistent manner. The *Privacy Officer* shall be responsible for the determination of appropriate sanctions and may involve human resources in any decision. In deciding upon the appropriate sanction, **Organization** may review the severity of the violation, the impact of the violation, and the *workforce member's* work history. The *Privacy Officer*, in his or her discretion, may review the sanction decision at the request of a *workforce member*.

Mitigation:
Organization must mitigate, to the extent practicable, any harmful effect that is known to it of a use or disclosure of *PHI* in violation of its policies and procedures or the *HIPAA* Privacy Rule by **Organization** or its *business associates*.

Organization will ensure that mitigation plans are developed, implemented and applied in accordance with these policies and procedures. In response to a report of or information about a *workforce member's* or *business associate's* unauthorized use or disclosure of *PHI*, **Organization** shall act promptly to reduce any known or reasonably anticipated harmful effects from the disclosure. **Organization** shall contact the recipient of the information that was subject of the unauthorized disclosure and request that such recipient either destroy or return the information. **Organization** will take other appropriate action to prevent further use or disclosure.

No Retaliation:
Organization will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against anyone who files a complaint either with the **Organization** or with *HHS*, who exercises a right to which they are entitled under the Privacy Rule, or the *Breach* Notification Rule, or who testifies, assists with or participates in an investigation, compliance review, or proceeding, or opposes any act or practice that he or she reasonably believes is unlawful under these regulations.

Waiver of Rights:
Organization will not require any *individual* to waive his or her right to file a complaint with **Organization** or *HHS*. Organization may not condition the provision of *treatment*, *payment*, enrollment in a health plan, or eligibility for benefits on an *individual*'s waiver of their right to file such a *HIPAA* compliance complaint.

Policies and Procedures:
The policies and procedures to be developed and reviewed by the *Privacy Officer* must comply with all Privacy Rule standards, implementation specifications, and requirements. These policies

and procedures must be reasonably designed, taking into account **Organization's** size and the type of activities that relate to *PHI* undertaken by **Organization**.

Changes to Policies and Procedures:
Organization must change its policies and procedures as necessary and appropriate to comply with changes in the law. Whenever a change in law necessitates a change to **Organization's** policies or procedures, **Organization** must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the Notice of Privacy Practices, **Organization** must change the contents of the notice accordingly. If the Organization has not retained the right to revise its Notice of Privacy Practice, it may *amend* the Notice, policies and procedures but the changes are only applicable to *PHI* created, received, maintained or transmitted prior to the effective date of the revision. **Organization** may not implement a change to a policy or procedure prior to the effective date of the revised notice.

Documentation:
Organization must maintain its policies and procedures in written or electronic form and must maintain all required documentation (which includes the policies and procedures, and any communications or actions the *HIPAA* Privacy Rule requires to be in writing) for six years from the date of its creation or the date when it was last in effect, whichever is later.

RELEVANT HIPAA REGULATIONS:

45 CFR Part 164 Subpart E
45 CFR 164.530 HIPAA Privacy Program Administrative Requirements

Privacy Policy 2.0 Administrative, Technical and Physical Safeguards of PHI

FULL POLICY LANGUAGE:

Policy Purpose:
It is the policy of **Organization** to ensure that *PHI* is protected from misuse, loss, tampering, or use by unauthorized persons. This policy addresses the safeguarding of *PHI* received, created, used, maintained, and/or transmitted and reflects some of the safeguards implemented by **Organization** to protect the privacy of *PHI*.

Policy Description:
The *HIPAA* Privacy Rule, 45 CFR 164.530, requires **Organization** to develop and implement safeguards to protect the privacy of *PHI*. This policy reflects the development of safeguards appropriate to Organization's operations and some of the safeguards **Organization** has implemented to protect the privacy of *PHI* that is not in electronic form. **Organization** has also implemented safeguards for the protection of *ePHI* as required concurrently by the Privacy Rule and the Security Rule. (The *HIPAA* Security Rule section 164.306(a) requires the safeguarding of

the confidentiality, integrity, and availability of *ePHI* that **Organization** creates, receives, maintains, or transmits). The *ePHI* safeguards are reflected in the Security Manual.

Procedures:

Organization will protect the privacy of *PHI*. In order to do so, **Organization** implements safeguards for the protection of *PHI* and *workforce members* are encouraged to make suggestions regarding and use additional safeguards that aid them in protecting the privacy of *PHI* that they *access* in the course of their role with the **Organization**.
Safeguards need not be complicated. They include things like putting away *PHI* when not in use, not keeping it where it is easily accessible to others, locking cabinets containing *PHI* and securing the keys. They are as simple as taking any Organization offered training and following the requirements, of all Policies and Procedures, understanding that it is your responsibility to follow them and that you are subject to discipline for not following the safeguards established.

When operations, facilities or circumstances change, **Organization** will promptly assess the new situation and develop and adapt safeguards appropriate to the circumstances if current safeguards will not sufficiently address the privacy of *PHI*. The Privacy or Compliance Officer or their designee and others involved in the management of the operations or facility that are new or changing will work together with the *workforce* to assure reasonable and appropriate safeguards are in place to protect the privacy and integrity of the *PHI*.

Safeguards **Organization** has established, and *workforce members* must follow include:

The Privacy and Security and other **Organization** Policies and Procedures including any Code of Conduct or ethics policies;

Directions of your supervisor or managers within the Organization related to the privacy of *PHI*.

Take and follow all training

Use common sense strategies to protect *PHI* from public view, incidental disclosure and harm or theft appropriate to the situation you are in (while speaking loudly in an ER to assure all clinical staff understands the patient's needs is appropriate, speaking loudly in a waiting room about the reason for a patient's visit is not)

Securely store all documents with *PHI* when they are not in use in locked cabinets or in sturdy boxes kept off the ground to avoid damage in a locked area or office

Shield *PHI* from public view

Follow faxing instructions including the use of the Organization's fax cover sheet, include a confidentiality notice on all fax cover sheets, do not use *PHI* on cover sheets, assure the person is expecting the fax, confirm the fax number, and periodically update any stored fax numbers;

The **Organization's** fax cover sheet will include the following details: fax cover sheets that include the following information: sender's name, facility, telephone and fax number; Date and time of transmission; Number of pages being faxed, including cover sheet; Intended recipient's name, facility, telephone and fax number; Name and number to call to report a transmittal problem or to inform of a misdirected fax.

Utilize first class mail for delivery services or other reliable delivery services such as UPS, FedEx, and DHL.

Utilize services such as certifying and tracking deliveries when signatures or proof of delivery are desirable or required.

Use packaging which protects the contents of a letter or package from view, assuring to use appropriately sized and quality packaging to protect *PHI* in transit;

Use sign-in sheets with only minimally necessary information to avoid or limit incidental exposure of a person's *PHI*

Respect signage that restricts *access* to certain areas of the facility

Do not ask for information orally if it can be provided in a form that will be less likely to expose the information. For example, ask for a copy of an insurance card rather than having the *individual* read their number aloud to you;

Always discuss *PHI* in a lowered voice and in a discreet manner or move to a more private area if circumstances allow if others without a need or right to have the information are present.

Never dispose of *PHI* in a wastebasket and always follow appropriate disposal methods for documents, films, recordings or other forms of *PHI* that include shredding or other means of rendering the information undecipherable

Lock doors, do not share keys, *access* codes or badges and secure them when not in use

Do not install video surveillance without full approval from the *Privacy Officer*

Protect the facility where *PHI* is present by installing smoke and heat detectors. Make sure to have fire extinguishers and fire suppressants on hand and operational. Assure any necessary sprinklers are automatic and in working order, Perform or require the landlord to perform necessary building maintenance.

Assure the facility is properly ventilated and clean to avoid damage from temperature humidity, dust and dirt

Always secure consent or authorizations prior to sharing information when they are required

Utilize an emergency power shutdown management system when appropriate

Require *workforce member* identification

Utilize sign and sign out sheets for all vendors entering the facility and assure and have them be accompanied as appropriate to assure privacy

Use common sense tactics to avoid theft, inadvertent exposure and damage to *PHI*

Make suggestions for changes or for more formal safeguards for recurring situations you may encounter

Use caution when addressing different envelopes at the same time, always check the address on correspondence with address on the envelope or label before sealing,

Organization will consider the appropriateness and feasibility of installing physical barriers, like walls, office cubbies, heavy curtains or soundproofing in areas where there is a high likelihood of potential incidental *access* to oral *PHI*.

Follow the *minimum necessary standard* whenever it applies.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.528(c): *Accounting of Disclosures of Protected Health Information: Safeguards*

Privacy Policy 3.0 Minimum Necessary Standard

FULL POLICY LANGUAGE:

Policy Purpose:

To establish rules for ensuring that Organization appropriate applies use of *Minimum Necessary Standard*s when requesting, using and disclosing protected health information.

Policy Description:

The *HIPAA* Privacy Rule generally requires *covered entities*, including **Organization**, to make reasonable efforts to adhere to a "minimum necessary" standard with respect to the request for, use and disclosure of *PHI*. When requesting, using or disclosing *PHI*, **Organization** shall make reasonable efforts to limit *PHI* to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request under circumstances where the standard applies.

Procedures:

Applicability of Standard:

The *minimum necessary standard* applies in many situations so *workforce members* must be aware of the situations in which it does not apply and act in accordance with the standard in all other circumstances. Accordingly, **Organization** and all *workforce members* will apply the Minimum Necessary standard for requesting, using and disclosing *PHI* except for requests, uses and disclosures made in the following circumstances:

1. Disclosures to or requests by a health care *provider* for *treatment* purposes;
2. Uses or disclosures made to the *individual* who is the subject of the information or their legal representative including those made pursuant to an *individual*'s request under the Privacy Rule Right of *Access* Standard (164.524), or the Accounting of *PHI* Disclosures Standard (164.528).
3. Uses or disclosures made pursuant to a valid and *HIPAA* compliant authorization (information provided in these circumstances will be limited by the terms of the authorization itself);
4. Disclosures made to the U. S. Department of Health and Human Services (*HHS*) when disclosure of information is required for enforcement purposes (i.e., in response to a complaint filed with the Secretary of *HHS*); and

5. Uses and disclosures that are required by law to the extent that the use or disclosure complies with and is limited to the relevant requirements of such law (i.e., victims of abuse; neglect or domestic violence; judicial administrative proceeding; and law enforcement purposes).

Procedure for Limiting *Access* When Standard Must be Followed:

1. **Organization** will identify the classes of persons or job titles within **Organization's** *workforce* who need *access* to *PHI* to carry out their job duties and responsibilities as described in **Organization's** job descriptions.
2. **Organization** will authorize *access* to computerized health information. Use of this information will be limited based on reasonable determination regarding an *individual*'s position and/or department.
3. Organization will control an individual's *access* via ID and password. The sharing of login IDs and passwords is prohibited.

Routine or Recurring Requests and Disclosures for *Individual*'s Information when the Standard Applies:

1. Requests for patient information made on a routine or recurring basis shall be limited to the minimum amount of the *individual*'s information necessary to meet the needs of the request/disclosure.
2. Organization will establish minimum necessary definitions and standard protocols for routine and recurring requests/disclosures (i.e., patient information that is routinely disclosed to a medical transcription service).
3. Organization will not be required to individually review requests/disclosures made on a routine or recurring basis where standard protocols have been developed; however, Organization will periodically review routine or recurring requests to ensure they are still valid and necessary.

Non-Routine Requests for Disclosure of *Individual*'s Information when the Standard Applies:

1. Organization will review non-routine requests for patient information on an individual basis to limit the patient information requested/disclosed to the minimum amount necessary to accomplish the purpose of the request/disclosure.
2. *Workforce members* will perform these reviews on an individual basis remembering that the standard does not apply to request/disclosure to or from a health care *provider* for *treatment* purposes.
3. *Workforce members* will not review disclosures/requests authorized by the *individual* or the *individual*'s legal representative for conformance with the *minimum necessary standard* but will review it for conformance with the terms of the authorization.
4. **Organization** may not use/disclose an entire *medical record* if it is determined, after conversation with the requestor or by established protocol, that the entire *medical record* is not justified as the amount that is reasonably necessary to accomplish the purpose of the use/disclosure.

Reasonable Reliance:

1. **Organization** may rely on the judgment of the party requesting the disclosure as to the minimum amount of information reasonably necessary for the stated purpose, in the following circumstances:
    a. Making permitted disclosures to public officials, if the public official presents that the information requested is the minimum necessary for the stated purpose(s);
    b. The *PHI* is requested by another *covered entity* (i.e., health care *provider*, health plan or health care clearinghouse);
    c. The *PHI* is requested by a professional who is requesting it for the purpose of providing professional services to **Organization** (requested is the minimum necessary for the stated purpose and is requested by a *member* of **Organization's** *workforce* or *business associate's workforce*; or
    d. The documentation or representations comply with the applicable provisions for using/disclosing *PHI* for *research* purposes and have been provided by a person requesting the information for such purposes (i.e., appropriate documentation from the *Institutional Review Board*).
2. **Organization** *workforce members* will exercise their own reasonable judgment/discretion when making determinations about disclosures in other circumstances where the *minimum necessary standard* applies and will limit the use, disclosure or request to the amount of information reasonably necessary to satisfy the purpose of the request.

Restrictions:
See Privacy Policy 16: *Individual Right: Request Restrictions and Alternate Confidential Communications* for *PHI* for more information regarding the availability of restrictions of communication of *PHI*. These restrictions must be met even in situations in which the *minimum necessary standard* applies.

Requesting Patient Information:
When requesting *PHI* from *covered entities*, **Organization** will limit any request for information to that which is reasonably necessary to accomplish the purpose for which the request is made. PHI requests made by *providers* for treatment purposes are not covered here, and the minimum necessary standard does not apply to their requests.

Corrective Action:
Upon determination of inappropriate or unauthorized *access* to or disclosure of *PHI* by a *workforce member*, the **Organization** will determine the appropriate corrective action for the misconduct and assess the matter as a Privacy incident. Please refer to Privacy Policy 1.0: *Privacy Program: General* regarding failure to comply with privacy practices, Privacy Policy 8.0: *Sanctions/Discipline* and Privacy Policy 6.0: *Incident Response and Reporting and Breach Determination* for further details on how to handle such matters.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.502(b)(1) *Minimum Necessary Standard*

45 CFR 164.514(d)(3) *Minimum Necessary Disclosures of Protected Health Information*
45 CFR 164.524(a) *Access to Protected Health Information*

Privacy Policy 4.0 Verification of Identity and Authority

FULL POLICY LANGUAGE:

Policy Purpose:

The purpose of this policy is to ensure the **Organization** fulfills the *HIPAA* requirement that identity and authority of persons seeking disclosure of a patient's protected health information (*PHI*) be verified before disclosure.

Policy Description:

To ensure that protected health information (*PHI*) is disclosed only to appropriate persons, **Organization** shall verify the identity and authority of a person making a request for the disclosure of *PHI* unless the *individual* has agreed to the disclosure. In addition, **Organization** will obtain from the person seeking disclosure of *PHI*, such documentation, statement, or representation, as may be required under the *HIPAA* Privacy Rule or desired as a best practice (and not prohibited by law), prior to a disclosure.

Procedures:

Organization will verify the identity and confirm the authority of any individua*l* outside of **Organization** requesting *PHI* if the identity of the person or the authority of the individual is not already known to the **Organization.** If the individual or their authority is known to the **Organization**, **Organization** may still elect to verify the identity periodically.

If documentation, statements or representations are a condition of disclosure under the Privacy Rule, Organization will obtain them prior to the disclosure. The details of any oral representation will be recorded in writing by the **Organization**.

When the Requester is the *Individual*:

When the requester is the *individual*, verification of identity may be accomplished by asking for photo identification (i.e., driver's license) if the request is made in person. If the request is made over the telephone or in writing, verification may be accomplished by requesting identifying information (i.e., address, telephone number, birth date, and/or *medical record* number) and confirming that this information matches what is in the *individual*'s record. If the *individual* is known to the person receiving the request, no identification verification is required. Organization still may verify identification of the *individual* in these circumstances if it chooses, especially when requests are not in person.

When the Requester is the *Individual*'s *Personal representative*:

Please also refer to Privacy Policy 11: *Uses and Disclosures of PHI, General Rules* paragraph on *Personal representative*s and Privacy Policy 20: *Minors' Rights* for specifics on *personal representative*s of minors.

When the Requester is the *individual*'s *personal representative*, verification of identity may be accomplished by asking for photo identification (i.e., driver's license) if the request is made in person. Once identity is established, authority in such situations may be determined by confirming the person is named in the *medical record* as the *individual*'s *personal representative*.

If there is no person listed in the *medical record* as the *individual*'s *personal representative*, authority may be established by the person presenting a copy of a valid power of attorney for health care or a copy of a court order appointing the person guardian (or guardian ad litem) of the *individual*. Authority may also be established by an *individual*'s identification of the person or by a relative (like a parent, spouse, friend or partner) by providing their identification along with information reflecting their relationship to the *individual*.

When the Requester is a Public Official or Law Office:
Please refer to Privacy Policy 22.0: *Uses and Disclosures: Response to Judicial and Administrative Proceedings* for more specifics of responding to requests related to Judicial and Administrative requests. In verifying the identity of a public official or law office (i.e., attorneys, judges, law enforcement officers, medical examiners, or coroners), **Organization's** *workforce* may rely on any of the following, if reasonable under the circumstances:

1. A badge or other credential.
2. A Bar association listing.
3. A request on government or law firm letterhead.
4. If the person making the request is acting on behalf of a public official, a written statement on government letterhead that the person is acting on behalf of the public official.

Once identity has been verified, when the public official or law office submits the request, whether in person or in writing, *workforce members* presented with, advised of, or who become aware of such requests, will alert their supervisor as soon as possible. The supervisor will then forward the request to the *Privacy Officer* of the **Organization.** Only the *Privacy Officer* or their designee may respond to the request unless legal process requires no delay.

The *Privacy Officer* or their designee, in consultation with others, including counsel, when assistance is needed, will establish the authority of the public official or legal process.

Organization may rely on the following, if reliance is reasonable under the circumstances:

1. A written statement of the legal authority or, if a written statement would be impracticable, an oral statement of such legal authority;

2. A request made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or *administrative tribunal* is presumed to constitute legal authority. Refer to Privacy Policy 22.0: *Uses and Disclosures: Response to Judicial and Administrative Proceedings* for more details on procedures.

If the public official's request is an administrative request, subpoena, or a request related to an investigation, the **Organization** shall disclose the requested *PHI*, provided the document containing the request, recites:

1. The information sought is relevant to a lawful inquiry, legal proceeding, investigation, or law enforcement activity.
2. The request is specific and limited in scope, as much as practicable, for the purposes of the inquiry.

When the Request is to Avert a Serious Threat to Health or Safety or in Situations allowing an *Individual* to Agree or Object:

HIPAA verification requirements are met where the Organization relies on the exercise of professional judgement when disclosing information in situations allowing an *Individual* to agree or object. See Privacy Policy 12.0; *Uses and Disclosures Requiring an Individual Opportunity to Agree or Object* for details of those situations.

HIPAA verification requirements are met where the Organization acts on a good faith belief in making a disclosure related to averting a serious threat to health or safety. See the paragraph addressing these disclosures in Privacy Policy 14.0: *Uses and Disclosures, No Authorization Required*, for further details on these disclosures**.**

When the Request is for *Research* Purposes:
If disclosure is sought for *research* purposes, pursuant to a waiver of authorization, the requesting documents must:

1. Show that the waiver of authorization has been approved by a properly constituted *Institutional Review Board* (*IRB*) or Privacy Board; and
2. Be signed by the Chair of the *IRB*, or that person's designee.

See the paragraphs covering *research* in Privacy Policy 14.0: *Uses and Disclosures: No Authorization or Right to Agree or Object Required* for further details.

Other Requesters:
Procedures for verifying the identity and/or authority of other unknown requesters of *PHI* will vary according to the circumstances. For example, if a person appears in person and is not known or recognized presents a written authorization by the *individual* as the basis for obtaining *PHI*, *workforce members* shall request that the person present photo identification to verify that the person is indeed the person named in the authorization to receive the *PHI*. See Privacy Policy 4.0: *Verification of Identity and Authority* for further details.

When Identity Has Not Been Clearly Established:
Generally, **Organization's** *workforce* may rely on required documentation, statements, or representations that, on their face, meet the verification requirements, provided the reliance is reasonable under the circumstances. If there are concerns as to the reliance, staff shall contact the *Privacy Officer* or their designee for guidance.
See Privacy Policy 4.0: *Verification of Identity and Authority* for further details.

RELEVANT *HIPAA* REGULATIONS:

45 CFR 164.514(h)(1) *Standard Verification Requirements*

Privacy Policy 5.0 Complaints to the Organization

FULL POLICY LANGUAGE:

Policy Purpose:
To provide an effective process for reporting concerns or complaints about **Organization's** privacy policies and procedures, **Organization's** compliance with those policies and procedures, and **Organization's** compliance with the *HIPAA* Privacy Rule and the *HIPAA Breach* Notification Rule. To prevent intimidating, threatening, coercing, discriminating against, or retaliating against any *individual* who has exercised a right under *HIPAA* including filing complaints.

Policy Description:
Organization strives to ensure the privacy of Protected Health Information ("*PHI*"), and to ensure this information is used and disclosed in accordance with all applicable laws and regulations and in conformance with the Privacy Manual. Organization will honor an *individual*'s right to make complaints concerning **Organization's** compliance with the *HIPAA* Privacy Rule, its Notice of Privacy Practices and its *HIPAA* privacy policies and procedures. Organization will honor an *individual*'s right to make complaints concerning the **Organization's** *breach* notification process and compliance with the *Breach* Notification Rule.

Organization will also act to prevent anyone from intimidating, threatening, coercing, discriminating against, or retaliating against any *individual* who has exercised their right under *HIPAA* to file complaints with the **Organization** concerning it's *HIPAA* compliance. Any such act that is reported to **Organization** will be investigated by the *Privacy Officer* or an uninvolved person designated by the **Organization** and handled under Privacy Policy 8.0: *Sanctions/Discipline* when appropriate.

When a Privacy complaint belongs to the subset of complaints referred to as Privacy Incidents - any attempted or successful unpermitted or unauthorized *access*, use, disclosure, modification, interference or destruction of *unsecured PHI* in any form - **Organization** will handle the

complaint according to Privacy Policy 6.0: *Incident Response and Reporting and Breach Determination.*

Procedures:

Processing a Complaint:

1. Organization's Notice of Privacy Practices must notify *individual*s (or their *personal representative*s) of their right to complain to Organization or the Department of Health and Human Services ("*HHS*").
2. Organization will accept complaints in person, by telephone, mail or email.
3. *Workforce members* should forward complaints received in any manner to the *Privacy Officer*.
4. Upon receipt of any complaint about **Organization's** privacy policies and procedures, **Organization's** compliance with those policies and procedures, and **Organization's** compliance with the *HIPAA* Privacy Rule and the *HIPAA Breach* Notification Rule, the *Privacy Officer* shall document the following in a *Complaint Log*:
    a. The date the complaint was received; and
    b. A copy of the written complaint, if any, or a general description of the verbal complaint.
5. Once the complaint is correctly documented in the Complaint Log, the *Privacy Officer* shall coordinate with appropriate individuals to determine whether the complaint is a Privacy incident. If it is a Privacy incident the complaint will be handled according to the process in Privacy Policy 6.0: *Incident Response and Reporting and Breach Determination*.
6. If the complaint is not a Privacy incident, the *Privacy Officer*, in coordination with other appropriate individuals, including counsel where necessary, shall decide whether an investigation is warranted. If an investigation is warranted, the *Privacy Officer* or their designee will conduct the investigation. The **Organization** will make reasonable efforts to complete the investigation in a timely manner.
7. If the complaint involves an allegation of intimidation, threats, coercion, discrimination against, or retaliation against any *individual* who has exercised their right under *HIPAA* to file complaints with the **Organization** concerning it's *HIPAA* compliance, the complaint will be investigated by the *Privacy Officer*, or an uninvolved person designated by the **Organization.**
8. If any person designated under this policy to investigate, receive or respond to complaints is a party to the action or inactions complained of, Organization will assign an uninvolved person with appropriate skill and knowledge to review, investigate and respond to the complaint.
9. Upon completion of complaint investigations under this policy, the *Privacy Officer* shall:
    a. Document the outcome of the complaint by entering the resolution and any required follow-up actions on the Complaint Log.
    b. Communicate the outcome of the complaint to the person who made the complaint within 30 days from the *Privacy Officer*'s receipt of the complaint.
10. If the *Privacy Officer* determines that a violation of policy, procedure, the *HIPAA* Privacy Rule, or the *HIPAA Breach* Notification Rule has occurred, the *Privacy Officer* shall

initiate and coordinate actions as appropriate according to **Organization's** *Sanctions Policy* (see Privacy Policy 8.0). **Organization** will develop and implement a corrective action plan to address the violation and mitigate any consequences of the violation.

11. The *Privacy Officer* shall maintain documentation of all complaints received, and the disposition of each, for a period of at least six years.

RELEVANT HIPAA REGULATION:

45 CFR 164.530(a)(d) and (g)*Administrative Requirements: Personnel Designations, Complaints and Refraining from Intimidating or Retaliatory Acts*
45 CFR 164.524(d) *Individual Right: Right to file Complaint Concerning Denial of Access*
45 CFR 164.520(b)(1)(vi) *Notice of Privacy Practice: Complaints*

Privacy Policy 6.0 HIPAA Incident Response and Reporting and Breach Determination

FULL POLICY LANGUAGE:

Policy Purpose:

Organization takes the privacy, security and integrity of *individuals'* data seriously. **Organization** also has legal responsibilities to protect *PHI* under *HIPAA*, to identify and respond to suspected incidents, mitigate harm, require its *workforce members* to report incidents, and to determine when there is a reportable *breach* of an *individual*'s *PHI*.

The purpose of this Incident Response and Reporting and *Breach* Determination Policy is to meet **Organization's** responsibilities and to provide guidance to Organization *workforce members* regarding recognizing and reporting a privacy or *security incident* involving Member health information. Organization will review all reported incidents and will follow the procedures set forth to determine if there has been a *Breach* (an acquisition, *access*, use, or disclosure of the Member's *unsecured PHI* in a manner not permitted under *HIPAA*).

Policy Description:

This policy establishes guidelines for Organization to

- Require the reporting of suspected privacy and *security incident*s (any attempted or successful unpermitted or unauthorized *access*, use, disclosure, modification, interference or destruction of *unsecured PHI* in any form). All *workforce members* must report any suspected incident to the Compliance, Privacy or Security Officer as soon as possible, and may report anonymously through The Guard if preferred. *Workforce members* who fail to promptly report incidents will be subject to discipline. See Privacy Policy 8.0: *Sanctions/Discipline* for additional details.
- identify and respond to suspected or known incidents involving the security or privacy of protected health information, including mitigating any harmful effects. Organization will handle any complaint that is potentially a privacy or *security incident* under this

Policy, which also appears in the Security Manual, instead of Privacy Policy 5.0: *Complaints to the Organization*.

- determine if there has been a *Breach* of *unsecured PHI* ("*PHI*") after analyzing potential exceptions and performing a risk analysis or requiring any involved *Business associate* to do so and then reviewing their determination, and
- document the incidents, responses and *Breach* determinations and retain the documentation for at least six years.

Procedures:

Reporting of *Security incident*s:
Organization will train all *workforce* Members on *HIPAA* privacy and security requirements. All Organization *workforce members* must report to their supervisor and/or Organization's Compliance, *Privacy Officer* or Security Officer as soon as possible and in no event later than 24 hours after discovering any suspected, known, or potential Privacy or *Security incident*. Supervisors must notify the Privacy and Security Officers immediately upon notification of potential, known or suspected Incidents. Organization *workforce members* are subject to discipline for failure to promptly report any suspected, known, or potential *Breach* of *unsecured PHI*.
Organization will require *Business associates* to report Privacy and *Security incident*s promptly and will enforce contract requirements.
Monitoring for Privacy and *Security incident*s:

Organization shall employ tools and techniques to monitor events, detect attacks and provide identification of unauthorized use of the systems that contain Electronic Protected Health Information (*ePHI*) and also periodically review *access*, integrity, use and disclosure of all *PHI*, in whatever form, to identify any potential *breach*es.
Treatment of Recurring and Expected Unsuccessful HIPAA incidents.

Organization acknowledges the ongoing existence or occurrence of attempted but "Unsuccessful *Security incidents*" including but not limited to, pings, and other broadcast attacks on firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above. As long as no such Unsuccessful *Security incident* results in unauthorized *access*, use or disclosure, inappropriate denial of *access* or harm to the integrity of *ePHI*, they will be reviewed, and the reports kept but Organization will not undertake a full factual investigation or *breach* determination analysis for each such unsuccessful attempt. Unsuccessful *Security incident*s will also be reviewed for heightened frequency and considered in the development, implementation of and improvements to safeguards. Organization will perform a thorough analysis of any suspicious circumstances or unusual activity found during reviews.
20904 Perform and Document a Factual Investigation of the Incident

Organization will perform a factual investigation of any reported potential privacy or *security incident*. At a minimum, [Organization] will seek information and documentation sufficient to

a) perform an analysis of whether there was any attempted or successful *unauthorized access*, use, disclosure, modification, or destruction of information in any form, b) determine if any unsecured information was involved, c) determine if any *PHI* was involved d) determine if any exception to an assumption of a *Breach* of *PHI* exists, e) perform the risk of *PHI* compromise analysis and f) determine the number of *individual*s impacted. If Organization has a separate investigations policy, it will follow that policy. Organization may retain outside resources for the completion of some or all of the investigation, especially if a forensic investigation is desirable.
Should the Privacy or *Security incident* occur through a *business associate*, [Organization] may rely on the *Business associate* to conduct an investigation but may also conduct an independent investigation if it so chooses. Organization must review the *Business associate's* findings and underlying facts prior to deciding on whether or not to rely solely on the *Business associate's* investigation or to perform its own investigation.

Determine Need and Implement Reasonable Mitigation Measures

Following the report or discovery of any HIPAA incident, Organization will assess whether any immediate or future safeguards or changes to process or practice are required to address the incident or its potential reoccurrence. Organization should determine whether to involve law enforcement on a case-by-case basis. For mitigations specific to *security incidents*, please refer to Security Policy 6 for examples.

20905 Determine if There Was Any Attempted or Successful Unauthorized *Access*, Use, Disclosure, Modification, or Destruction of Information in Any Form

Following a standard procedure and utilizing the HIPAA Breach Risk Assessment Record and *Unsecured PHI* Job Aid or similar documentation when applicable, Organization will determine whether a) there was any attempted or successful *access*, use, disclosure, modification or destruction of information, b) whether the information involved was unsecured, c) whether such information was *PHI* or *ePHI*, d) whether such *access*, use, disclosure, modification, or destruction was unauthorized or unpermitted and e) whether any exceptions to a determination of a *breach* is applicable.

Organization will use the Unsecured PHI Job Aid or a similar standard assessment tool to determine if any information involved in the incident was unsecured.

Organization will determine if the information involved in the attempted or successful unauthorized *access*, use, disclosure, modification, or destruction of information was *PHI*. For example, if the information involved a deceased *individual*, Organization will determine if the *individual* been deceased for more than fifty years.
Organization will determine if *access*, use, disclosure, modification, or destruction was unauthorized or unpermitted by determining if the use or disclosure was authorized or permitted under *HIPAA*. For example, Organization will determine if it was authorized by the *individual*, required by law, or permitted as incidental.

Determine if there is an Applicable Exception to a *Breach* Determination

As part of its *breach* determination, Organization will refer to the three exceptions listed in paragraph 1 of the definition of *Breach* published in 45 CFR § 164.402 to analyze whether an exception applies for the fact pattern of the Privacy or *Security incident*. Organization will determine and record its determination as to whether any of these three exceptions applies to the incident:

Any unintentional acquisition, *access*, or use of protected health information by a *workforce member* or person acting under the authority of a *covered entity* or a *business associate*, if such acquisition, *access*, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part (Sets forth allowable uses of *PHI*). Example, when someone at a *business associate* was looking for a record, they needed to perform their responsibility and inadvertently accessed Mary B's record instead of Mary A's record and did not further disclose information from Mary B's record, this exception applies.

Any inadvertent disclosure by a person who is authorized to *access* protected health information at a *covered entity* or *business associate* to another person authorized to *access* protected health information at the same *covered entity* or *business associate*, or organized health care arrangement in which the *covered entity* participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part (Part E sets forth allowable uses of *PHI*). Example, Dr. Brown requested an *individual*'s record to perform his job responsibilities, but Mary delivered the record to Dr. Black instead. So long as all of them work at the same CE, BA or within an organized health care arrangement and Dr. Black did not further disclose the information, there is no *breach*.

A disclosure of protected health information where a *covered entity* or *business associate* 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. Example, a nurse hands the wrong discharge papers to a patient and notices the error right away, taking back the papers.

If an exception applies, Organization will record its findings in the incident record and the incident can be closed. If no exception applies, there is a presumption that a *breach* has occurred. Organization may either perform a risk analysis according to the procedure set forth below or forego performing that analysis and follow the process for notifications under Privacy Policy 7.0: *Breach Notification*.

Perform an Analysis of Risk of Compromise to *unsecured PHI* utilizing the Four Required Factors and Other Pertinent Information

If Organization has determined that there is a presumption of a *breach*, Organization may perform a risk of compromise assessment using at least the following four required factors to determine if there is a low probability that *PHI* has been compromised that rebuts the presumption of a *breach*:

The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

The unauthorized person who used the protected health information or to whom the disclosure was made;

Whether the protected health information was actually acquired or viewed; and

The extent to which the risk to the protected health information has been mitigated. Organization may also consider other factors in its analysis that might support a finding of a low probability of risk including but not limited to the time the information may have been accessible or accessed, the likelihood the information was accessed, whether any complaints were received, how difficult or likely *access* was even if there was accessibility and any professional or legal requirements applicable to the person who received the information (does a legal privilege apply, was the person who received the information in healthcare and trained on *HIPAA* privacy requirements). The *HIPAA* Incident Assessment Tool may be useful in completing and documenting the risk of compromise assessment.
If the *Breach* occurred through a *business associate*, Organization may rely on a *business associate* to perform the risk of compromise assessment but must review the findings and underlying facts prior to deciding on whether to perform its own assessment.

Record Keeping
Organization will create and maintain a *HIPAA* incident log for all reported incidents, regardless of whether they are determined to be *Breach*es. Organization shall review this log periodically to determine areas that may require additional training. Organization will keep records concerning all reports of security or privacy incidents, any finding of an exception to the *Breach* definition, all analyses of risk of compromise to *unsecured PHI*, and the factual investigations and documentation supporting the analysis and findings. These records will be kept for a minimum of six years following the conclusion of the *Breach* determination for the incident(s). Where Organization has found an applicable exception to a *Breach* or made a finding of a low probability of compromise to *PHI*, Organization's records must sufficiently demonstrate the application of any exception or support a finding that there is a low probability of compromise to the *PHI*.

Enforcement and Reporting
Organization's Compliance Officer and Organization's *HIPAA* Privacy and Security Officers or their designees, along with human resources, are responsible for managing, updating, and enforcing this policy. Violations of this policy must be immediately reported.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.308(a)(6)(i) *Security Incident Procedures*
45 CFR 164.308(a)(6)(ii) *Implementation Specification: Response and Reporting (Required)*
45 CFR 164.530(a)(c)(e)(f) *Administrative Requirements: Personnel Designations, Safeguards, Sanctions and Documentation, Mitigation*
45 CFR 402 *Definitions: Breach*

Privacy Policy 7.0 Breach Notification

FULL POLICY LANGUAGE:

Policy Purpose:

Organization takes the privacy and integrity of an *individual*'s personal health information seriously. Organization also has legal responsibilities to protect *PHI* under *HIPAA*, to determine when there is a reportable *breach* of an *individual*'s *PHI* and to make appropriate and timely notifications following a *breach*.

The purpose of this *Breach* Notification Policy is to meet Organization's responsibilities and to provide guidance to Organization *workforce members* regarding making required notifications when a *Breach* determination has been made under Privacy Policy 7.0: *Breach Determination*.

This policy establishes guidelines for Organization to

- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to *individual*s impacted by a *Breach*,
- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to federal and state authorities if required by the details of the *Breach* determination,
- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to media if the findings of the *Breach* determination require them;
- Determine when and if appropriate substitute notice is allowed and to use that substitute notice when appropriate; and
- Document compliance with the requirements of *Breach* notifications.

Policy Description:

This policy establishes guidelines for Organization to

- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate timely notifications to *individual*s impacted by a *Breach*;
- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate timely notifications to federal and state authorities if required by the details of the *Breach* determination including reporting of *breach*es involving less than 500 *individual*s in a single state or geographic region to *HHS* electronically on an annual basis by March 1 (or February 29th in a Leap year) of the year following the *Breach*;
- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate timely notifications to media if the findings of the *Breach* determination require them;
- Determine when and if appropriate substitute notice is allowed and to use that substitute notice if required or desired;
- Ascertain and meet any more stringent applicable contractual notification requirements; and
- Document compliance with the requirements of this policy.

Following the determination of a *breach* under Privacy Policy 9: *HIPAA incident Reporting and Response and Breach Determination* **Organization** will determine what external notifications

are required or should be made (i.e., Secretary of Department of Health & Human Services (*HHS*), media outlets, law enforcement officials, etc.), develop appropriate content for the notices, reports and postings, and communicate each notification, report or positing according to the procedures and requirements set forth below.

Procedures

Privacy and Security Officers Shall Direct all Notifications but may appropriately Delegate Activities

With input from the Compliance Officer and others at their discretion, Organization's Privacy and Security Officers will direct all activities required under this policy including the wording of any *Individual* Notices, *HHS* filings, communications required by contract, Media notices, and scripts (including escalation processes) for any telephone inquiries. Legal representation will be utilized if desired by the Privacy or Security Officer or at the direction of anyone on the senior leadership team of the Organization. The Privacy and Security Officer may delegate responsibilities as appropriate but remain responsible for the implementation of *Breach* Notification Policy requirements. This delegation includes allowing either another responsible *Covered entity* or a responsible *Business associate* to make the notifications. Organization remains responsible for assuring all requirements have been met by the delegated entity or individual. For responsibilities of *Business associates*, please refer to Privacy Policy 9.0: *Business associates* for more information.

Organization will Determine Notification Requirements based on the findings of the *Breach* Incident Investigation

Organization will use the Number of *Individual*s Involved to Determine Appropriate Notifications and Timing.

Individual Notification: If the number of *individual*s impacted by a *breach* is known to be less than 500, Organization will follow the notification Procedures set forth below for the timing and content of *Individual* Notification and Notification to *HHS*.

500 or More: If the number of *individual*s affected by the *Breach* is known to be 500 residents of a State or jurisdiction, Organization will provide notification to Prominent media outlets serving the State and regional area where the impacted *individual*s reside and follow the notification Procedures set forth below for the timing and content of Media Notice, *HHS* and Notification for *Breach*es Affecting more than 500 *individual*s.

If the number of *individual*s is uncertain, Organization must use reasonable efforts to estimate the number of affected *individual*s and document its methods. Organization shall use this estimate to determine the number of *individual*s affected for determining appropriate notification procedures. Should further information or investigation prove the estimate to be incorrect, Organization must update any previous notifications or reports made using that estimate if the method or content of the Notice is materially different due to the change.

See Chart below for Summary of Requirements. Details of Appropriate Notice, Timing, Content and Means appear below the summary chart.

IF	Notification To	Timing*	Content	Means of Notice
Number of *Individuals* impacted is less than 500	Each person individually	Without unreasonable delay and in no case later than 60 days following discovery of *breach*	In plain language A. A brief *breach* description, including date and the date of B. types of *unsecured PHI* that were involved C. steps the *individual* should take to protect themselves D. what the organization is doing to investigate, mitigate harm to *individuals*, and to protect against further *Breach*es; and E. Contact procedures	In writing by first class mail or by email if the affected *individual* has consented to such notice. Additional notice in urgent situations, it may do so by telephone or other means in addition to the written notice Substitute notice**
	HHS	no later than 60 days after the end of the calendar year in which the *Breach*es were discovered (March 1 or February 29th in a leap year).	In addition to content required for *individual* notice, Information Required on Current *HHS* report includes Entity Contact, BA Contact if Occurred at BA, Number of *individuals* impacted, safeguards placed prior to *breach*, mitigation efforts, safeguards placed after *breach*, number of *individuals* impacted	Completion of online form on the *HHS* website
Number of *Individuals* Impacted is greater than 500 in any State or jurisdiction	Prominent Media Outlet serving the areas where impacted *individuals* reside	without unreasonable delay and in no case later than 60 days following the discovery of a *Breach*	In plain language: A. A brief *breach* description, including date and the date of B. types of *unsecured PHI* that were involved C. steps the *individual* should take to protect themselves D. what the organization is doing to investigate, mitigate harm to *individuals*, and to protect against further *Breach*es; and E. Contact procedures	Contact media and provide information to be included in publication

	HHS	without unreasonable delay and in no case later than 60 days following the discovery of a *Breach*	In addition to content required for media notice, Information Required on Current *HHS* report includes Entity Contact, BA Contact if Occurred at BA, Number of *individuals* impacted, safeguards placed prior to *breach*, mitigation efforts, safeguards placed after *breach*, number of *individual*s impacted	Completion of online form on the *HHS* website

*Subject to Law Enforcement requests for delay
**Substitute notice may be used in some situations for *individuals*, see policy for details.

Timing

Organization will provide *Individual* notice without unreasonable delay and in no case later than 60 days following the discovery of a *Breach*. The Organization may also provide additional notice in urgent situations because of possible imminent misuse of the *PHI*.
Organization will provide Media Notice, when required, without unreasonable delay and in no case later than 60 days following the discovery of a *Breach*.
Organization will provide *HHS* notice by completing a web report form on the following timeline: If 500 or more individual residents of a State or jurisdiction are affected, Organization will complete the *HHS* notification without unreasonable delay and in no case later than 60 days following the discovery of a *Breach*. If fewer than 500 *individual*s are affected, Organization will notify *HHS* of each *Breach* no later than 60 days after the end of the calendar year in which the *Breach*es were discovered (March 1 or February 29th in a leap year).

Discovery of *Breach*:
A *breach* of *PHI* shall be treated as "discovered" as of the first day the *breach* is known to the **Organization**, or, by exercising reasonable diligence would have been known to the **Organization** (includes *breach*es by **Organization's** *Business associates*). The **Organization** shall be deemed to have knowledge of a *breach* if such *breach* is known or if by exercising reasonable diligence would have been known, to any person, other than the person committing the *breach*, who is a *workforce member* or an *agent* of the Organization (i.e., a *Business associate* acting as an *agent* of the **Organization**).

Delays in timing permitted: Law Enforcement Delay

When Organization is notified by a law enforcement official that a notification, notice or posting required for a *Breach* would either impede a criminal investigation or damage national security, Organization may delay the notification, notice or posting for a) a period of time specified by the law enforcement official in writing or b) for the requested amount of time not to exceed 30 days from the date of an oral request for delay from a law enforcement official. Organization

will extend the original 30-day delay imposed by an oral request if a law enforcement official makes a later request in writing prior to the expiration of the initial delay request. Any such oral or written request must be documented by Organization and the record preserved. *Workforce members* should also refer to Privacy Policy 4: *Verification of Identity and Authority* when processing any law enforcement request for delay.

Content and Means of Notifications and Postings

At a minimum the content of reports, notifications and notices required by law for *breach*es of the privacy or security of *PHI* in any form must include the information set forth below and must be communicated by the means indicated:
Individual Notice: Means of Communication

In writing by first class mail or by email if the affected *individual* has consented to such notice. Reference the Sample Breach Notification format for all *Individual* Notice. If the Organization desires to send additional notice in urgent situations, it may do so by telephone or other means in addition to the written notice but not as a substitute for it.

Substitute *Individual* Notice

When Organization has insufficient contact information for ten or greater affected *individual*s, Organization will give notice by posting notice for 90 days on the company website or by publication in major print or broadcast media in the area where the affected *individual*s likely reside.
When Organization has insufficient contact information for fewer than ten affected *individual*s it may give notice to those *individual*s by alternative written notice, by telephone or other reasonable means.

Individual Notice: Content

1. A brief description of what happened, including the date of the *Breach* and the date of the discovery of the *Breach*, if known;
2. A description of the types of *unsecured PHI* that were involved in the *Breach* (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3. Any steps the *individual* should take to protect themselves from potential harm resulting from the *Breach*;
4. A brief description of what the **Organization** is doing to investigate the *Breach*, to mitigate harm to *individual*s, and to protect against further *Breach*es; and
5. Contact procedures for *individual*s to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

Media Notice Means of Communication and Content

For Media Notices the following information should be included and the Notice must include enough information for an *individual* to determine whether their information may have been disclosed, what they should do if it was and who to contact for more information:

1. A brief description of what happened, including the date of the *Breach* and the date of the discovery of the *Breach*, if known;
2. A description of the types of *unsecured PHI* that were involved in the *Breach* (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3. Any steps the *individual* should take to protect themselves from potential harm resulting from the *Breach*;
4. A brief description of what the **Organization** is doing to investigate the *Breach*, to mitigate harm to *individual*s, and to protect against further *Breach*es; and
5. Contact procedures for *individual*s to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

Means of Notifying *HHS*

For a *Breach* Affecting 500 or More *individual*s Organization will timely complete a Notice utilizing the form on the *HHS* website (https://*OCR*portal.hhs.gov/*OCR*/*breach*/wizard_*breach*.jsf?faces-redirect=true).
For a *Breach* Affecting less than 500 *Individual*s Organization will timely file (within 60 days of the end of the calendar year in which the *Breach occurred*) a Notice utilizing the form on the *HHS* website (https://*OCR*portal.hhs.gov/*OCR*/*breach*/wizard_*breach*.jsf?faces-redirect=true).

Reliance on Others to Provide Notification.

Organization will determine any contractual obligations related to the *PHI*. If allowable, Organization may choose to rely upon notifications given by a *Business associate* for the *Breach* notifications required. Organization will request copies of any notifications to its *individual*s, the public and *HHS* if Organization's *individual*'s information was *breach*ed.

Record Keeping

Organization must keep records concerning all notifications, notices and postings made separately for each *Breach* reported. This includes any reports, notices or postings made by any other party on which Organization relied for its own notice to *individual*s, agencies, authorities, or media. These records must be kept for a minimum of six years following the provision of the notice, report or posting. If desired, utilize the *Breach* Notification Documentation Job Aid to record the details for recordkeeping.

RELEVANT HIPAA REGULATIONS:
45 CFR 164.404 *Notification to Individuals*

45 CFR 164.406 *Notification to the Media*
45 CFR 164.408 *Notification to the Secretary*
45 CFR 164.410 *Notification by a Business Associate*
45 CFR 164.412 *Law Enforcement Delay*
45 CFR 164.414 *Administrative Requirements and Burden of Proof*
45 CFR 164.530 *Administrative Requirements*

Privacy Policy 8.0 Sanctions/Discipline

FULL POLICY LANGUAGE:

Policy Purpose:

To ensure that appropriate sanctions will be applied to *Workforce members* who violate the requirements of the *HIPAA* Privacy Rule, **Organization's** *HIPAA* privacy policies and procedures, the *HIPAA Breach* Notification Rule and/or **Organization's** *HIPAA Breach* Notification Rule policies and procedures. **Organization** must develop and apply appropriate sanctions against *workforce members* who fail to comply with its privacy policies and procedures and/or the *HIPAA* Privacy Rule. **Organization** must document all sanctions and apply them in a consistent manner. The *Privacy Officer* shall be responsible for the determination of appropriate sanctions and may involve human resources in any decision. In deciding upon the appropriate sanction, **Organization** may review the severity of the violation, the impact of the violation, and the *workforce member's* work history. The *Privacy Officer*, in his or her discretion, may review the sanction decision at the request of a *workforce member*

Policy Description:

It is **Organization's** policy to impose sanctions, as applicable, for violations of **Organization's** policies and procedures regarding *workforce member HIPAA* compliance. **Organization** will develop and apply appropriate sanctions against *workforce members* who fail to comply with its privacy policies and procedures and/or the *HIPAA* Privacy Rule. **Organization** must document all sanctions and apply them in a consistent manner. The *Privacy Officer* shall be responsible for the determination of appropriate sanctions and may involve human resources in any decision. In deciding upon the appropriate sanction, **Organization** may review the severity of the violation, the impact of the violation, and the *workforce member's* work history. The *Privacy Officer*, in his or her discretion, may review the sanction decision at the request of a *workforce member*

Organization will not impose discipline against any *workforce member* or *Business associate* for disclosing *PHI*, if the person believes in good faith either that **Organization** has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care or services provided by **Organization** potentially endanger one or more *individual*s, workers, or the public; **and** the disclosure is either to a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct of **Organization.**

Procedures:

Sanctions:
Workforce members who violate Organization's privacy policy and procedures are subject to sanctions. Sanctions are disciplinary measures intended to address violations and to deter future violations. **Organization**, in deciding upon the appropriate sanction, may review the severity of the violation, the impact of the violation, and the *workforce member's* work history. Sanctions imposed will be consistent, and proportional with the severity of the offense. Discipline up to and including termination, even for first violations, may be appropriate.

Following the report or discovery of a *HIPAA* incident, the *Privacy Officer*, in conjunction with the Human Resources team when appropriate, will initiate discipline against any *workforce member* who was found to have violated the requirements of the *HIPAA* Privacy Rule, **Organization's** *HIPAA* privacy policies and procedures, the *HIPAA Breach* Notification Rule and/or **Organization's** *HIPAA Breach* Determination/Notification Rule policies and procedures.

Upon receipt or report of an allegation that an *individual* has been subjected to intimidation or retaliation, the *Privacy Officer* shall investigate, and upon conclusion of the investigation, shall impose appropriate sanctions. See Privacy Policy 1.0: *HIPAA Privacy Program: General* for a discussion of prohibited intimidation and retaliation.

Fair and Consistent Discipline
The *Privacy Officer* shall uniquely and consistently apply corrective disciplinary action when warranted, up to and including termination of employment or contracts. Whenever appropriate, progressive discipline will be applied. Sanctions imposed will be consistent, and proportional with the severity of the offense with like violations under similar fact patterns treated equally.

Facts and Circumstances that May be Considered in Making Disciplinary Decisions
Organization will consider the type and severity of the violation, factors that mitigate or increase the appropriate sanction and any other pertinent facts relative to the violation at issue.

Type of Offense	**Examples**
Willful Intentional Violation	Disclosure of Celebrity *PHI* to Tabloid, Sale of *PHI*, Identity theft
Violation with Harmful Intent	Malice, disclosure of a condition of a rival; Disclosure of a Mental Health condition
Deliberate Violation without harmful intent (Curiosity)	Looking up a friend's *medical record*s
Failure to Follow Policies and Procedures	Violation due to poor job performance such as not seeking appropriate authorization before releasing records, leaving detailed *PHI* on a voicemail
Accidental or Inadvertent Violations	Violations due to human error such as misdirecting a letter or email

Factors to consider that Might Mitigate or Increase Appropriate Sanction

Violation included sensitive information *Records included Mental health Condition, Substance Abuse Records*
High volume of data impacted *An entire record was impacted rather than one encounter, many records were involved*
High number of *individuals* impacted
Breach resulted from violation
Organization incurred significant expense as a result of the violation *Organization bore the expense of an extensive investigation and breach notification*
Harm to a patient resulted from the violation
Workforce member was not forthcoming or honest during investigation
Workforce member reported the incident themselves
History of Performance Issues for Individual
Failure of Training Individual *had not been offered all training before violation occurred*
Action taken at request of individual in authority
Training Understood but ignored
Long Job Performance, exemplary employee

Examples of Appropriate Types of Discipline to Consider

Organization will consistently impose appropriate sanctions for violations. The penalty should be more stringent for repeat offenses and intentional or malicious violations. Sanctions and discipline up to and including termination of employment of contracts may be appropriate even for first violations.

Types of Discipline to Consider (on an Escalating Scale)

Verbal or Written Reprimand
Retraining on Privacy/security awareness
Retraining on privacy security policies and procedures
Retraining on Proper Use of Forms
Letter of Reprimand
Probationary status
Suspension
Unpaid Leave
Final Waring
Longer term Suspension
Termination of Employment or Contract

Appeals:

1. In the event that a sanction triggers any process of appeal under an applicable **Organization** disciplinary policy and procedure, the *workforce member* is entitled to file an appeal. The *Privacy Officer* or other appropriate individual shall review the appeal, which shall be in writing, and shall render a decision upon such appeal.
2. In the event that the party hearing the appeal is not authorized by **Organization** or *HIPAA* regulations to *access PHI*, the identity of the *individual* whose privacy rights were

violated shall be removed to the extent feasible or, if that is not possible, other measures must be taken to ensure *HIPAA* compliance prior to providing the party with *PHI*.

Documentation of Disciplinary Actions

1. **Organization** shall document all disciplinary action, including:
    a. All information about the nature of the violation;
    b. The names and roles of the parties who played a role in determining the disciplinary action;
    c. The facts and circumstances considered in determining the disciplinary action (without regard to whether such considerations were relied upon in determining the disciplinary action);
    d. The discipline imposed (including lack of discipline);
    e. The nature of the appeals process used, if any, and the results thereof; and
    f. The actions taken in order to enforce the discipline.
2. Such documentation shall be retained in accordance with **Organization's** document retention policies, and, in any event, for no less than six years.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.530(e) *Sanctions*

Privacy Policy 9.0 Business Associates

FULL POLICY LANGUAGE:

Policy Purpose:

The purpose of this policy is to meet **Organization's** responsibility to determine whether a vendor is a *business associate* as defined by the *HIPAA* regulations. and to provide rules for creation, content, maintenance, and termination of *business associate agreement*s that establish protections for the privacy and accessibility of protected health information created, received, maintained, or transmitted on **Organization's** behalf and meet the requirements of the Privacy Rule.

Policy Description:

It is the policy of the Organization to determine which of its vendors are *business associates*, to enter into *Business associate agreement*s containing all the required elements to protect the privacy of health information, to provide rules for creation, maintenance, and termination of *Business associate agreement*s, and to provide for rules regarding the use and disclosure of information and the reporting of uses or disclosures not provided for in the *Business associate agreement*.

A *business associate* is an individual or entity that provides a service, performs a function, or performs an activity on behalf of a *covered entity* that involves the creation, receipt, maintenance or transmission of protected health information, including but not limited to claims processing or administration, clinical staffing, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, repricing, legal representation and accounting. *Business associates* do not include *members* of the **Organization's** *workforce*. A *Business associate agreement* is a legally binding contract, in which, the *business associate* provides, in writing, satisfactory assurances that it will appropriately safeguard the information it creates, receives, maintains or transmits in carrying out specified functions or activities for a *covered entity* as well as agreeing to provide *access* and *amendment* to records, and reporting of *breach*es and incidents. **Organization** may only disclose protected health information (*PHI*) to a *business associate* after a valid *business associate agreement* is in place.

Procedures:

20404 *Business associate* Determination:

Organization shall inventory all outside business and service vendors to determine if they are *business associates*. For a vendor to be considered a *business associate*, the following requirements must be met:

- The vendor/business' staff *members* are not *members* of **Organization's** *workforce*;
- The vendor/business is performing a function, service or activity on behalf of the **Organization**;
- That "something" involves the *access* to, creation, receipt, maintenance or transmission of *PHI*.

To make the *business associate* determination, **Organization** will inventory all existing business and service vendors to determine if they are *business associates*. It will also make such a determination for any new vendors engaged by Organization prior to entering into an agreement for services, function or activity with the vendor.

Organization will enter into *Business associate agreement*s for all vendors identified as *Business associates* unless the circumstances discussed below in Other Requirements for Contracts and other Arrangements apply.

***Business Associate* Contracts/Agreements:**

If an entity is determined to be a *business associate* must require a *business associate agreement* that provides in writing satisfactory assurances that it will appropriately safeguard the information it receives, uses, or discloses in carrying out the specified functions or activities.

The satisfactory assurances obtained from the *business associate* must, at a minimum, contain the provisions specified in the Privacy Rule, provisions that:

1. Establish the permitted and required uses and disclosures of protected health information by the *business associate* and not allow the *business associate* to further use or disclose information in manner that would violate the Privacy Rules except that a *business associate* may use or disclose information
    a. for the proper management and administration of the *business associate*; and
    b. to provide *data aggregation* services relating to healthcare operations of the *covered entity*;
2. Provide that the *business associate* will not use or further disclose the information other than as permitted or required by the contract or as required by law;
3. Require the *business associate* to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the *HIPAA* Security Rule regarding electronic protected health information. Such safeguards include administrative, technical and physical safeguards.
4. The BAA shall require the *business associate* to train its *workforce* on the *HIPAA* Security Rule, and on the provisions of the *HIPAA* Privacy Rule with which *Business associate* must comply in the performance of the agreement with the *covered entity*.
5. Require *business associate* to timely report to the *covered entity* any use or disclosure of the information not provided for by its contract of which it becomes aware, including *breach*es of *unsecured PHI*. Organization will handle any reported information in a timely manner according to its policies on *Breach* Determination and Notification. Organization may also require the *business associate* to determine whether a use or disclosure of information not provided for by the agreement is a *breach* on behalf of the *covered entity*, to document its rationale for the *breach* determination, or a contrary determination, and to send and/or pay for the expense of any notifications required as a result of the non-allowed use or disclosure of the information.
6. Ensure that any subcontractors of *business associate* that create, receive, maintain or transmit protected health information on behalf of the *business associate* agree to the same restrictions and condition that apply to the *business associate* with respect to such information;
7. Require the *business associate* to disclose protected health information as specified in its contract to satisfy **Organization's** obligation with respect to *individual*s' requests for *access* or copies of their protected health information
8. Make protected health information available for *amendment* and incorporate any *amendment*s as required or when appropriate, if allowed under the 45 CFR 164.526;
9. Make available the information required for an *accounting of disclosures*;
10. To the extent the *business associate* is to carry out **Organization's** obligation(s) covered under the Privacy Rule, the agreement must require the *business associate* to comply with the requirements that apply to the *covered entity* in the performance of the obligation;
11. Require the *business associate* to make available to *HHS* its internal practices, books, and records relating to the use and disclosure of protected health information received from, created, or received by the *business associate* on behalf of **Organization** for purposes of *HHS* determining **Organization's** compliance with the *HIPAA* Privacy Rule;

12. At termination of the contract, if feasible, require the *business associate* to return or destroy all protected health information received from, created, or received by the *business associate* on behalf of **Organization** that it still maintains in any form and retain no copies of such information, or, if destruction is not feasible, extend all of the protections of the contract to the information and limit further use and disclosures of such information to those purposes that make return or destruction of the information infeasible; and
13. Authorize termination of the contract by the **Organization** if the *business associate* violates a material term of the contract as determined by the Organization. This term may be omitted if it is inconsistent with statutory obligations of either the Organization or its *business associate*.

Other requirements for Contracts and Other Arrangements

If the Organization and its *business associate* are both governmental agencies than it may substitute the performance of these responsibilities under the substitute rules set forth at 45 CFR 504(e)(3)(i).

If a *business associate* is required by law to perform a *covered entity* function or activity or provide a covered service, **Organization** may disclose protected health information to that entity without the necessity of entering into a *business associate agreement* if the Organization attempts in good faith to obtain satisfactory assurances and if it is unable to do so documents its attempts and the reasons why the assurances cannot be obtained.

If the Organization and the *business associate* enter into a Data Use Agreement that meets the requirements set forth at 45 CFR 164. 514(e)(4) and 164.314(a)(1), if applicable, the Organization is in compliance with the Privacy rule if it only discloses a *limited data set* to the *business associate* for them to carry out a healthcare operation function.

In the Event of Material *Breach* or Violation or a Pattern or Practice that violates the *Business associate agreement*:

The Organization should monitor *business associates* for patterns or practices that violate the requirements of their *business associate agreement*. It should address all such patterns or practices with *business associate* to assure the *business associate* takes steps to end the violation.

If **Organization** knows of a material *breach* or violation by the *business associate* of the contract or agreement, the **Organization** is required to assure *business associate* takes reasonable steps to cure the *breach* or end the violation.

If such steps are unsuccessful, the **Organization** must terminate the contract or agreement. If termination of the contract or agreement is not feasible, the **Organization** must report the problem to the Secretary of the Department of Health and Human Services (*HHS*).

Workforce members shall immediately notify the **Organization's** *Privacy Officer* if and when they learn that a *business associate* may have *breach*ed or violated its *business associate agreement*.

***Business associates*: Required and Permitted Uses and Disclosures:**
If **Organization** is acting as a *business associate* it must follow these rules when acting in that capacity and will require its *business associates* to follow these requirements.

A *business associate* of **Organization** may use or disclose *PHI* only as permitted or required by its *business associate agreement* with the **Organization**.

1. A *business associate* may not use or disclose *PHI* in a manner that would violate the Privacy Rule, if done by the **Organization**, except:
    a. If the *business associate* contract permits the business to use and disclose protected health information for the proper management and administration of the *business associate*; or
    b. If such uses or disclosures are lawfully permitted by the *business associate agreement*.
2. A *business associate* is required to disclose *PHI*:
    a. When required by the *HHS* Secretary to investigate or determine the *business associate's* compliance with *HIPAA*.
    b. To the **Organization**, if the *PHI* is the subject of a request for *access* and is maintained in electronic *designated record set*s. Under such circumstances, if an *individual* requests an electronic copy of such information, the *business associate* must provide the **Organization** with *access* to the *designated record set*s, so that the **Organization** can provide the *individual* (or the *individual*'s designee) with the requested *access*.

RELEVANT HIPAA REGULATIONS:

45 CFR 160.103 *Business Associate Definition*
45 CFR 164.502(a)(3)-(4) *Permitted and Required Uses and Disclosures; Business Associates*
45 CFR 164.504(e) *Standard Business Associate Contracts*

Privacy Policy 10.0 Notice of Privacy Practices

FULL POLICY LANGUAGE:

Policy Purpose:
*Individual*s are entitled to adequate notice of the uses and disclosures of protected health information and of the *individual*'s rights and the Organization's responsibilities with respect to *PHI* unless an exception applies. The Privacy Rule requires **Organization** to describe its privacy

practices in plain English, in a document called a Notice of Privacy Practices ("Notice"). **Organization** must give *individual*s a copy of this document.

Policy Description:

Organization must timely make its Notice available to all *individual*s and post the Notice throughout its facilities and on its website. **Organization** must also make a good faith effort to obtain written acknowledgements from patients that they have received the Notice. The Notice must contain all of the required elements notifying an *individual* of the permitted uses and disclosures; uses and disclosures that require an opportunity for them to agree or object; uses and disclosures that require an authorization; whether the **Organization** intends to use or disclose information for marketing, facility directories or *fundraising*; the *individual*'s rights to *access*, *amendment*, and limitations on sharing; the **Organization's** responsibilities; a way to make complaints; contact details for further information; and an effective date.

Procedures:

Notice Content Requirements:

The Notice shall contain the following content:

1. **Header:** The Notice must contain the following language as a header or otherwise prominently displayed:
    a. "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."
2. **Uses and Disclosures:** This part of the notice must contain:
    a. A description, including at least one example of the types of uses and disclosures of information that the **Organization** is permitted to make for each of the following purposes: *treatment*, *payment*, and *health care operations*;
    b. A description of each of the other purposes (other than *Treatment*, *Payment*, or *Health care operations*) for which the **Organization** is permitted or required to use or disclose *PHI* without the *individual*'s written authorization;
    c. If a use or disclosure otherwise allowed under paragraphs a and b above is materially limited or prohibited by a stricter law, the description of the use or disclosure must reflect the more stringent law;
    d. The description of the use or disclosures allowed under paragraphs a and b above must include sufficient detail to place the *individual* on notice of the uses and disclosures that are permitted or required by applicable law;
    e. A description of the types of uses and disclosures that require an authorization including *psychotherapy notes*, some marketing, sale of protected health care information, and a statement that other uses and disclosures not described in the Notice will be made only with the *individual*'s written authorization and that the *individual* may revoke this authorization at any time in writing which will be effective except to the extent the Organization has acted in reliance on it; and
    f. If Organization intends to use information in any of the following ways and is

the type of *covered entity* mentioned, it must include a separate statement in the Notice for each of the following activities: (i) *Covered entity* may contact *individual*s for *fundraising* activities and the *individual* has a right to opt out; (ii) a group health plan, health insurance issuer or HMO may share *PHI* to the plan sponsor; or (iii) a non-long term care health plan may use information for underwriting purposes, excluding the use of genetic information.

3. ***Individual* Rights**: The Notice must contain a statement of the *individual*'s rights with respect to *PHI*, and how he or she may exercise the right to:
    a. Request restrictions on certain uses and disclosures of information (the notice must contain a statement that the **Organization** is not required to agree to all requested restrictions);
    b. Receive confidential communications of *PHI*;
    c. Inspect and copy *individual*'s *PHI*;
    d. Seek *amendment* of *individual*'s *PHI*;
    e. Receive an *accounting of disclosures* of *individual*'s *PHI*; and
    f. Obtain a paper copy of the Notice of Privacy Practices upon request even if an electronic copy has already been provided.
4. **Organization's Duties**: The Notice must include statements of the following:
    a. **Organization** is required by law to maintain the privacy of protected health information, to provide *individual*s with notice of its legal duties and privacy practices with respect to protected health information, and to notify affected *individual*s following a *breach* of *unsecured PHI*;
    b. **Organization** must abide by the terms of the Notice currently in effect; and
    c. If Organization desires to reserve the right to *amend* the Notice, the Notice must state that **Organization** reserves the right to change the terms of its Notice and to make the new Notice provisions effective for all *PHI* it maintains. This statement must explain how the **Organization** will provide *individual*s with a revised Notice.
5. **Complaints**: The Notice must explain that *individual*s may file a complaint with the **Organization** and/or the Secretary of *HHS* if they believe their privacy rights have been violated. A brief description of how to file a complaint with the **Organization** must be included. The Notice must also include a statement that the *individual* will not be retaliated against for filing a complaint.
6. Contact Information. The Notice must contain the name, or title, and telephone number of a person or office to contact for further information.
7. Effective Date. The Notice must contain an effective date that is not earlier than the date it is published.

Notice Dissemination and Publication Requirements:

1. The **Organization** must provide the Notice to *individual*s no later than the date of the first service delivery by a direct care *provider*. The Notice may also be given to an *individual* by e-mail, if the *individual* agrees to such electronic notice. If the

Organization knows that the e-mail transmission has failed, it must provide a hard paper copy. If the first service is delivered electronically, the **Organization** must send the notice electronically, and contemporaneously with provision of the service.

2. The **Organization** must make the Notice available for *individual*s to take with them. (When the *individual* is not physically present, the Notice may be sent by first class mail.).
3. The Notice must be posted in a clear and prominent location where it is reasonable to expect *individual*s to be able to read the Notice.
4. The Notice shall be posted prominently on the **Organization's** website and shall be available electronically through the website.
5. If the Organization is a health plan, it must follow the requirements as set forth at 45 CFR 520(c)(1).
6. If the Organization participates in an organized health care arrangement it may comply with the Notice requirements by a joint Notice if it meets the requirements of 45 CFR 520(d).

Special Notice Requirements:

1. No Notice is required to be given to inmates who may receive *treatment* at an **Organization** facility.
2. In the case of patients who are minors, the Notice should be given to the minor's parent or guardian.
3. If Organization is a group health plan, Notice shall be available directly from the group health plan if the group health plan is uninsured or if it creates or receives *PHI* in addition to summary plan information, participation information or enrollment information. If the group health plan provides benefits through an insurer or HMO and does not receive the above information, then Notice is provided through the insurer or HMO.

Optional Elements.

1. If an **Organization** elects to limit its use and disclosure beyond the required limitations, it may describe the more limited use and disclosures although it may not limit uses and disclosures required by law or allowed to the *individual*.
2. The Organization must reserve its right to revise its Notice to change its limited uses for any information created or received prior to the revision.

Acknowledgement of Notice of Privacy Practices:

1. The **Organization** must make a good faith effort to obtain a written Acknowledgement that the *individual* received the **Organization's** Notice. If an *individual* refuses to sign the Acknowledgement, then the **Organization** must document the good faith efforts taken and the reason why the Acknowledgement was not obtained.
2. A "good faith effort" to obtain written acknowledgment is not required when emergency *treatment* or stabilization is required. In addition, if **Organization** mails the notice to the correct address, and the patient does not return the acknowledgment

form, the **Organization** does not need to make further good faith efforts to obtain a written acknowledgment.
3. In non-emergency situations, **Organization** will seek to obtain acknowledgement of the Notice during the intake process.

Revisions to the Notice of Privacy Practices:

1. The **Organization** must promptly revise and distribute its Notice whenever there is a material change to privacy practices, including practices regarding *PHI* uses and disclosures, *individual*'s rights, and **Organization** legal duties, or other privacy practices stated in the Notice.
2. **Organization** must make the revised notice available upon request.
3. **Organization** must post the Notice in service delivery areas.
4. **Organization** must post the revised notice on its website.
5. Unless Organization reserved the right to *amend* its Notice within the Notice, it may not make any changes applicable to *PHI* created or received prior to the effective date of the new Notice**.**

Record Retention:

All versions of the **Organization** approved Notice of Privacy Practices will be archived and maintained by the *Privacy Officer* for a period no less than six (6) years from the date of its creation or the date when it was last in effect, whichever is later. Any acknowledgments of receipt or good faith efforts to obtain such acknowledgements must also be retained no less than six (6) years from the date when it was received or the date when it was last in effect, whichever is later.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.520 *Notice of Privacy Practices for protected health information*

Privacy Policy 11.0 Uses and Disclosures: General Rules

FULL POLICY LANGUAGE:

Policy Purpose:

To outline the general rules for when and how **Organization** can use or disclose *PHI* with more detail included in the policy sections referred to within this policy.

Policy Description:

It is the policy of this **Organization** to only use or disclose protected health information as permitted or required under the Privacy Rule and rules regarding compliance with the Privacy rule. *Workforce members* should be trained on and understand the circumstances in which use, or disclosure of *PHI* is permitted or required and should seek clarification from their Supervisor

of the *Privacy Officer* before sharing information if they are unsure what is permitted or required to be used or shared.

Organization will not use or disclose information in circumstances where use and disclosure is allowed unless all the administrative requirements applicable to that use or disclosure (examples include agreement of the *individual*, authorization, or confirmation of a legal requirement to disclose) have been met.

Organization may *request* consent but *will not condition* the provision of services or insurance on provision of consent or authorization for use or disclosure of *PHI* for *treatment*, *payment* or operations.

Organization will not condition provision of *treatment* or *payment* except as specifically allowed. Accordingly, **Organization** will not condition provision of *treatment*, *payment*, health plan enrollment, or eligibility of benefits on the signing of an authorization except as allowed in specific circumstances for *research*, health plan enrollment, or creation of phi to be disclosed to a third party.

Procedure:

Permitted Uses and Disclosures:

Organization *may* (i.e., is permitted under law) use or disclose protected health information as follows:

1. To the *individual*.
2. To its own *workforce* and other parties, for the purposes of *treatment*, *payment*, or *health care operations* of the Organization (see Privacy Policy 13.0: *Uses and Disclosures: No Authorization or. Right to Agree or Object Required* paragraphs on use of *PHI* for *Treatment*, *Payment* and *Health care operations*)
3. Incident to a use or disclosure that is otherwise permitted, provided **Organization** complies with the requirements of this Policy 11.0: *General Rules for Uses and Disclosures*; Privacy Policy on *Minimum Necessary Standard* (See Privacy Policy 3.0: *Minimum Necessary Standard*) and the requirements of Privacy Policy 2.0: *Administrative, Technical and Physical Safeguards of PHI* and any other policy that applies in the specific circumstances.
4. Pursuant to, and in compliance with, a valid written authorization (see Privacy Policy 15.0: *Individual Right: Access to Protected Health Information* and Privacy Policy 13.0 *Uses and Disclosures: Authorization Required and Requirements for Valid Authorization* for details). Use of genetic information for underwriting purposes remains prohibited.
5. Pursuant to an agreement under, or as otherwise permitted by, Privacy Policy 16.0: *Individual Right: Request Restrictions and Alternate Confidential Communications*. When **Organization** agrees to a restriction pursuant to Privacy Policy 16.0: *Individual Right: Request Restrictions and Alternate Confidential Communications*, **Organization** may not use *PHI* covered by the restriction in violation of that restriction.
6. As permitted by any applicable rule or regulation.

Required Uses and Disclosures:
Organization *must* (i.e., is required to, under the law) and will disclose *PHI*:

1. To an *individual*, pursuant to that *individual*'s request under the Privacy Rule Right of *Access* Standard (45 CFR 164.524), or the Accounting of *PHI* Disclosures Standard (45 CFR 164.528). See Privacy Policy 15.0: *Individual's Right to Access Protected Health Information* and Privacy Policy 18.0: *Individual Right: Accounting of disclosures* for further details.
2. When required by the *HHS* Secretary to investigate or determine **Organization's** compliance with *HIPAA* and the Privacy Rule. (45 CFR 160.310).

***Business associates* required and Permitted Uses and Disclosures:**
If **Organization** is acting as a *business associate* it must follow specific requirements when acting in that capacity and should require its *business associates* to follow these requirements. Refer to Privacy Policy 9's section on *Business associates*: Required and Permitted Uses and Disclosures for details.

Prohibited Uses and Disclosures:
Organization is prohibited from using and disclosing *PHI*, as follows:

Prohibited: Sale of Protected Health Information

Organization may not and will not sell protected health information, unless **Organization** obtains a valid written authorization for the disclosure of *PHI* for that purpose. A sale of *PHI* occurs when one party remunerates another, directly or indirectly, in exchange for the second party's giving *PHI* to the first party. When **Organization** seeks authorization for sale of *PHI*, the authorization must state that the disclosure will result in remuneration or *payment* to the **Organization**. For further details about valid authorizations for use of *PHI* for the sale or marketing of information and what is included and excluded from *HIPAA*'s definition of sale and marketing of *PHI*, refer to the paragraphs on sale and marketing within Privacy Policy 13.0: *Uses and Disclosures: Authorization Required and Requirements for Valid Authorization*.

Prohibited: Use and Disclosure of Genetic Information for Underwriting Purposes
Health plans: If **Organization** is acting in the capacity of a health plan, either in a primary or secondary capacity, it will not use or disclose *PHI* that is genetic information for underwriting purposes. Underwriting purposes include rules for, or determination of, eligibility for, or determination of, benefits under a health plan or policy; computation of premium amounts; the application of a pre-existing exclusion; and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits. Underwriting does not include determinations of medical appropriateness for *individual*s seeking a benefit under a plan, coverage or policy.

Minimum Necessary Standard

When using, disclosing or requesting information Organization must apply the *Minimum Necessary Standard* by making reasonable efforts to limit protected health information to *the minimum necessary* to accomplish the intended purpose of the use, disclosure or request. except when the standard does not apply. The *minimum necessary standard* does not apply to disclosures to the *individual*, those that are *required* under the Privacy Rule, those that are *required* under a law (like a response to a valid warrant or subpoena or the reporting of child abuse), and those that are made with an *individual*'s written authorization. See Privacy Policy 3.0: *Minimum Necessary Standard* for full details.

Uses and Disclosures: Agreed Upon Restriction

Organization will not use or disclose information in violation of a restriction it has agreed to unless required to do so (for example by a valid subpoena or the need to avert harm to the public or an *individual*). For further details on **Organization's** policy and procedure concerning requested restrictions see Privacy Policy 16.0: *Individual Right: Request Privacy Restrictions and alternate Confidential Communications* for *PHI*.

De-Identified *PHI*: Creation, Use and Disclosures:

1. **Organization** may use *PHI* to create information that is not *individually identifiable health information* or disclose protected health information to a *business associate* for the purpose of de-identification, whether or not the *de-identified information* is to be used by **Organization**.
2. If Organization decides to de-identify information, it will use an entity or *individual* with the required or desired expertise to assure it is done correctly and in accordance with the standard and implementation specifications for de-identification under 45 CFR 164.514(a) and 45 CFR 164.514(b).
3. Organization may use and disclose appropriately *de-identified information* outside of the protections of the *HIPAA* Privacy Rule provided that:
    a. Disclosure of a code or other means of record identification designed to enable coded or otherwise *de-identified information* to be re-identified constitutes disclosure of protected health information.
    b. If *de-identified information* is re-identified, **Organization** may use or disclose such re-identified information only as permitted or required by the Privacy Rule.

Disclosures to *Business associates* (See above for Use and Disclosure *by Business associate* and also Privacy Policy 9.0: *Business Associates***)**

Organization may disclose protected health information to a *business associate after* obtaining satisfactory assurances that it will appropriately safeguard the information. **Organization** will follow Privacy Policy 9.0: *Business Associates* in all its dealings with *business associates*.

Organization is not required to receive satisfactory assurances of appropriate safeguards to information directly from *business associates* that are subcontractors and may rely on the assurances the subcontractor *business associates* provide to **Organization's** direct *business*

associates. **Organization** may provide information to subcontracted *business associates* directly or through *business associates* after assurances have been given.

Deceased *Individuals*:
The *HIPAA* Privacy Rule applies to the *PHI* of a deceased *individual* for a period of 50 years following the person's death. During the 50-year period of protection, the Privacy Rule generally protects a decedent's health information to the same extent the Rule protects the health information of living *individual*s.

The Privacy Rule includes a number of special disclosure provisions relevant to deceased *individual*s. The following disclosures may be made within the 50-year period following the patient's death:

1. To alert law enforcement to the death of the *individual*, when there is a suspicion that death resulted from criminal conduct.
2. To coroners or medical examiners and funeral directors.
3. For *research* that is solely on the protected health information of decedents.
4. To organ procurement **Organizations** or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation.
5. To a family *member* or other person who was involved in the *individual*'s health care or *payment* for care prior to the *individual*'s death, unless doing so is inconsistent with any prior expressed preference of the deceased *individual* that is known to **Organization**.

For disclosure of *PHI* of a deceased person that is not covered under those enumerated above, **Organization** will obtain written consent from an authorized representative for disclosure to be permitted. Refer to the paragraph on deceased *individual*'s *personal representative*s below to determine who is authorized.

***Personal representatives*:**

Organization will treat a *personal representative* as the *individual* for purposes of the Privacy Rule with some exceptions to this general rule regarding unemancipated minors and circumstances involving suspected or known abuse, neglect and endangerment. When deciding how to use and share a minor's *PHI*, *workforce members* must first refer to Privacy Policy 20.0: *Minors' Rights* for more specific direction. For *personal representative*s of deceased *individual*s see last paragraph below.

Organization may decide not to treat an *individual* as a *personal representative* in situations of known or suspected violence, abuse, neglect or endangerment, even if other laws dictate that it is appropriate or required to treat an *individual* as a *personal representative*. In order for the **Organization** to elect *not to treat* a person as a *personal representative*, *workforce members* must document that

1. Organization, exercising professional judgment, decides it is not in the best interest of the *individual* to do so ***and***
2. Organization has a reasonable belief that ***either***
    a. the *individual* has been or may be subjected to domestic violence, abuse or neglect by that person; or
    b. treating the person as the *individual*'s *personal representative* will or could endanger the *individual*.

If, under applicable law, a parent, guardian, or other person acting *in loco parentis* has the authority to act on behalf of an unemancipated minor in making decisions related to healthcare, **Organization** will usually treat that person as a *personal representative* with respect to *PHI* relevant to such personal representation with exceptions for circumstances suggesting endangerment, violence, abuse or neglect as above and where the minor has rights that give them the authority to act as an *individual* with respect to *PHI* pertaining to health care services. Before deciding how to use and share a minor's *PHI*, *workforce members* must first refer to Privacy Policy 20.0: *Minors' Rights* for more specific direction.

If, under applicable law, an executor, administrator, or other person has authority to act on behalf of a deceased *individual* or of the *individual*'s estate, **Organization** must treat that person as the deceased's *personal representative*.

Confidential Communications:

Organization must comply with the applicable requirements of 45 CFR 164.522(b) in communicating *PHI*. Organization must permit *individual*s to request and must accommodate reasonable requests by *individuals* to receive communications of *PHI* by alternative means or at alternative locations. See Privacy 16.0**:** *Individual Right: Request Restrictions and Alternate Confidential Communications* for *PHI* for more details on how Organization handles and when it agrees to such requests.

Uses and Disclosures Consistent with Notice

Organization may not use or disclose *PHI* in a manner that is inconsistent with **Organization's** Notice of Privacy Practices. If it intends to engage in *fundraising* activities, **Organization** will not use or disclose *PHI* for *fundraising* without including a "*fundraising* notice" in its Notice of Privacy Practices. Refer to Privacy Policy Privacy 10.0**:** *Notice of Privacy Practices* for more details and additional information on other Notice of Privacy Practice requirements that might apply.

Uses and Disclosures: More Stringent Federal or State Law

Organization must be aware and comply with privacy and confidentiality requirements, including administrative requirements like obtaining specific *individual* authorization, from sources other than HIPAA. HIPAA does not preempt, and accordingly **Organization** will follow,

stricter federal and state requirements applicable to an *individual's PHI.* Examples of where stricter requirements are often present include state mental health record protections (in addition to HIPAA's strict psychotherapy record requirements), substance use disorder (SUD) records, including sharing for treatment purposes (see federal SAMSHA guidance), rules regarding public health activities, rules regarding gender reassignment and rules specific to deceased individuals and minors.

Use and Disclosure: Whistleblowers
Organization will allow use and disclosure of an *individual*'s information by *Business associates* and *workforce members* who believe in good faith that **Organization,** or a *member* of its *workforce*, is acting in violation of any law or a professional or clinical standard, or there is potential danger to *individual*s, workers or the public from care, services or conditions allowed by the **Organization**. Further details on circumstances where such uses and disclosure are allowed are found in Privacy Policy 14.0: *Uses and Disclosures: No Authorization or Right to Agree or Object Required*.

Use and Disclosure: *Workforce* Victims of Crime:
Organization will allow *workforce members* who are victims of a crime related to their work with **Organization** to disclose protected health information about the suspected perpetrator of the criminal act to law enforcement, provided the information disclosed is limited as described in Privacy Policy 14.0: *Uses and Disclosures, No Authorization or Right to Agree or Object Required.*

RELEVANT HIPAA REGULATIONS:

45 CFR 164.502 *Uses and Disclosures of Protected Health Information: General Rules*
45 CFR 164.501 *Definitions*
45 CFR 160.203 *General Rule and exceptions*

Privacy Policy 12.0 Uses and Disclosures Requiring Individual an Opportunity to Agree or Object

FULL POLICY LANGUAGE:

Policy Purpose:
To meet Organization's responsibility under several circumstances, to only use or disclosure *PHI* after an *individual* has been given the opportunity to agree or to prohibit or restrict the use or disclosure and to inform *workforce members* of the situations under which an *individual* must be given an opportunity to agree or object and how to meet the requirements.

Policy Description:
Under several circumstances, before **Organization** may use or disclose an *individual*'s *PHI*, the *individual* must be given an opportunity to agree or object to the use or disclosure:

1. use and disclosure of *PHI* by the Organization for purposes of a *facility directory*,
2. disclosure of *PHI* to a person that is directly relevant to that person's involvement with an *individual*'s care including *payment* for that care,
3. limited disclosure for notification of an *individual*'s location, general condition or death,
4. uses and disclosures for disaster relief purposes and
5. uses and disclosures when an *individual* is deceased (prior prohibition on disclosures must be honored).

It is the policy of the **Organization** that it will meet its responsibility to provide *individual*s the right to agree or object to uses and disclosures as required. Under each of these circumstances there are additional administrative requirements that must be met such as what to do if the *individual* is not present, when it is appropriate to exercise professional judgment and what is allowed in emergency circumstances that may not be allowed in the absence of an emergency. Special requirements that might apply in situations involving minors or other requirements like disclosures made pursuant to legal process may override the rights of an *individual* to agree or object. For details on such requirements please see the various Privacy Policies addressing those circumstances: Privacy Policy 20: *Minors' Rights*; Privacy Policy 22.0: *Uses and Disclosures: Response to Judicial and Administrative Proceedings*: Privacy Policy 11.0: *Uses and Disclosures: General Rules*.

Any *workforce member* who is unsure of appropriate use or disclosure should contact their supervisor or the *Privacy Officer* for direction prior to making a disclosure. *Workforce member* should follow the procedures below.

Procedures:

Uses and Disclosures Requiring an Opportunity for the *Individual* to Agree or to Object:
The **Organization** may use or disclose *PHI*, provided that the *individual* is informed in advance of the use or disclosure and has the opportunity to agree to, or prohibit/restrict the use or disclosure, in accordance with the applicable requirements set forth below.

The **Organization** may orally inform the *individual* of and obtain the *individual*'s oral agreement or objection to a use or disclosure permitted by this section. *Workforce members* should note any oral objection or agreement in the *individual*'s record.

Workforce members must afford an *individual* the opportunity to agree or object to a use or disclosure in the following circumstances:

1. use and disclosure of *PHI* by the Organization for purposes of a *facility directory* if the Organization is currently using one,
2. disclosure of *PHI* to a person that is directly relevant to that person's involvement with an *individual*'s care including *payment* for that care,
3. limited disclosure for notification of an *individual*'s location, general condition or death,
4. uses and disclosures for disaster relief purposes and
5. uses and disclosures when an *individual* is deceased (prior prohibition on disclosures must be honored).

If an *individual* expresses a desire to prohibit the use or disclosure, Organization will record that objection in the record and abide by that request. If the *individual* desires to restrict the disclosure in some way, for example not to disclose their religious affiliation to anyone but allowing disclosure of their general condition, the Organization will record that restriction in the *individual*'s record and abide by that request. *Workforce members* will review any objections or prohibitions in the record or ask the *individual* (if they are available) before using or disclosing information in the circumstances defined above.

*Individual*s may change their decision. For any use or disclosure made after the *individual* has changed their decision, Organization will abide by any new restrictions or prohibitions or any new agreement to a use or disclosure with an understanding that there may be a slight administrative delay in implementing some changes. If a *workforce member* anticipates a delay, they will notify the *individual* of the possibility (example inclusion in a *facility directory* after a previous request to be excluded – Organization will make a good faith effort to implement inclusion, but it cannot be done simultaneously with the decision.)

Uses and Disclosures for Involvement in the *Individual*'s Care and Notification Purposes:
Permitted uses and disclosures to those involved in the *individual*'s care or *payment* for their care and for notification purposes:

1. The **Organization** may disclose to a family *member*, other relative, or a close personal friend of the *individual*, or any other person identified by the *individual*, the *PHI* directly relevant to such person's involvement with the *individual*'s health care or *payment* related to the *individual*'s health care.
2. The **Organization** may use or disclose *PHI* to notify or assist in the notification of (including identifying or locating), a family *member*, a *personal representative* of the *individual*, or another person responsible for the care of the *individual* of the *individual*'s location, general condition, or death.

When *Individual* is Present.
Uses and disclosures to those involved in the *individual*'s care or *payment* for their care when the *individual* is present: If the *individual* is present for, or otherwise available prior to, a use or disclosure to those involved in the *individual*'s care or *payment* for their care and has the capacity to make health care decisions, the **Organization** may use or disclose the *PHI* if it:

1. Obtains the *individual*'s agreement;
2. Provides the *individual* with the opportunity to object to the disclosure, and the *individual* does not express an objection; or
3. Reasonably infers from the circumstances, based on the exercise of professional judgment that the *individual* does not object to the disclosure.

When *Individual* is not Present, Limited Use or Disclosure.
If the *individual* is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the *individual*'s incapacity or an emergency

circumstance, the **Organization** may disclose information using professional judgment in some circumstances and may also use knowledge of common practices in others.

1. Use of Professional judgment is appropriate, to determine whether the disclosure is in the best interests of the *individual*. and, if so, disclose only the *PHI* that is a) directly relevant to the person's involvement with the *individual*'s care or *payment* related to the *individual*'s health care or b) needed for notification purposes.
2. Use of Professional judgment and Experience with Common practice is appropriate to make reasonable inferences of the *individual*'s best interest in allowing a person to act on behalf of the *individual* in the following circumstances: to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of *PHI*.

Uses and Disclosures for Disaster Relief Purposes

The **Organization** may use or disclose *PHI* to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities. The uses or disclosures must only be to notify or assist in the notification of (including identifying or locating), a family *member*, a *personal representative* of the *individual*, or another person responsible for the care of the *individual* of the *individual*'s location, general condition, or death. Any such disclosure must respect the *individual*'s right to agree or object to such disclosure, including a) respecting any request for restricted use made prior to an *individual*'s death and b) following the process for use and disclosure for notification purposes when 1) the *individual* is present and 2) when the *individual* is not present as set forth above.

Uses and disclosures when the *individual* is deceased

If the *individual* is deceased, the **Organization** may disclose to a family *member*, or other persons identified in this section who were involved in the *individual*'s care or *payment* for health care prior to the *individual*'s death, *PHI* of the *individual* that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the *individual* that is known to the **Organization**.

Use and Disclosure for Facility Directories:

If the Organization is using, or desires to use, a *Facility directory*, it will do so only in agreement with the following requirements and procedures:

1. **Permitted uses and disclosure**. *Except when an objection is expressed*, the **Organization** may:
    a. Use only the following *PHI* to maintain a directory of *individual*s in its facility:
    b. The *individual*'s name;
    c. The *individual*'s location in the **Organization's** facility;
    d. The *individual*'s condition described in general terms that does not communicate specific medical information about the *individual*; and
    e. The *individual*'s religious affiliation; and
    f. Use or disclose the above information for directory purposes in the following manner:
    g. Members of the clergy will be given full directory information;

h. Any person asking for the *individual* by name will be given all directory information except religious affiliation.

2. **Opportunity to object**: The **Organization** will inform an *individual* of the *PHI* that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the *individual* with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by this section. Organization will notify appropriate *workforce members*, note any objections in the *individual*'s record and will not use or disclose information in a *facility directory* when an *individual* has objected to such use except as otherwise allowed, for example in response to a judicial order.
3. **Emergency circumstances**:
    a. If the opportunity to object to uses or disclosures cannot practicably be provided because of the *individual*'s incapacity or an emergency *treatment* circumstance, the **Organization** may use or disclose some or all of the *PHI* permitted in a *facility directory*, if such disclosure is:
    b. Consistent with a prior expressed preference of the *individual*, if any, that is known to the **Organization**; and
    c. In the *individual*'s best interest as determined by the **Organization**, in the exercise of professional judgment.
    d. The **Organization** will inform the *individual* and provide an opportunity to object to uses or disclosures for directory purposes when it becomes practicable to do so.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.510 *Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object*

Privacy Policy 13.0 Uses and Disclosures: Individual Authorization Required and Requirements for a Valid Authorization

FULL POLICY LANGUAGE:

Policy Purpose:

Organization will obtain and require valid written *individual* authorization before it uses or discloses information in the circumstances described in this policy and as required under the Privacy Rule.

Policy Description:

Generally, **Organization** may not use or disclose *PHI* without a valid written authorization from the *individual* who is the subject of the information, unless otherwise allowed under the Privacy Rule. When the *individual* provides a valid authorization, Organization's use and disclosure of the information must be consistent with the authorization. *Workforce members* must be familiar with the requirements of a valid authorization and the situations which require that

authorization be obtained prior to use or disclosure of information and must follow the terms of the authorizations that are in place. See Privacy Policy 19.0: *Use and Disclosure: No Authorization or Right to Agree or Object* for more detail on situations in which an authorization is not required.

Organization allows revocation of authorizations in writing with some minor exceptions as further detailed below. Organization will provide *individual*s with a copy of their authorizations. Organization will use and accept only valid authorization forms written in plain language which contain all the core elements and required statements for an authorization and will limit the use of compound authorizations to circumstances where they are allowed as detailed below. The **Organization** will also document and retain any signed authorization.

Organization will not condition the provision of *treatment*, *payment*, enrollment in a health plan, or eligibility for benefits on the provision of an *individual*'s authorization except in limited circumstances as allowed under the Privacy Rule and further described below.

Organization will meet the requirements for authorizations related to the sale of *PHI* and communications for marketing purposes.

Procedures:

Use only Valid Authorization Forms

Organization will use and accept only valid written authorization forms meeting the authorization requirements below. Organization will not accept any authorizations that include a defect as listed in the defective authorizations section below. Organization will only use and accept compound authorizations in situations allowed under the Privacy Rule as described below in the Compound Authorization section.

Authorization Requirements

A valid authorization under *HIPAA* must be written in plain language and contain at a minimum the 6 core elements defined in the Privacy Rule and at least 3 required statements. A fourth statement is required if the authorization relates to either the sale of *PHI* or the use and disclosure of *PHI* for marketing purposes. The content of this fourth statement is specific to either marketing or sale of *PHI*. Organization will require that all authorizations that it uses or accepts will contain all the required element and statements.

Workforce members will be aware of these validity requirements and not use or disclose information under an authorization that is not valid. If a *workforce member* has questions about the validity of any specific authorization or form, they should make their supervisor or the *Privacy Officer* aware as soon as possible. Supervisors should answer *workforce member* questions posed to them with oversight and input from the *Privacy Officer*. *Privacy Officer* may use necessary additional resources to determine the validity of an authorization.

Privacy Officer will periodically review authorization forms used or accepted by Organization on a regular basis to assure they are valid and will review any new authorization form to be used by *workforce members* to obtain authorizations before they are made available for use.

Core Elements and Requirements
Generally, each authorization must contain a description of the information to disclose, who is authorized to disclose it, who is authorized to receive it, the purpose for the disclosure (or notation that it is at *individual*'s request), when it expires, and a signature. These core elements are set forth in more detail below.

Core Elements: A valid authorization will contain at least the following elements (but may contain additional information so long as it does not create an inconsistency in the document):

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
3. The name or other specific identification of the person(s), or class of persons, to whom the **Organization** may make the requested use or disclosure;
4. A description of each purpose of the requested use or disclosure. The statement "at the request of the *individual*" is a sufficient description of the purpose when an *individual* initiates the authorization and does not, or elects not to, provide a statement of the purpose;
5. An expiration date or an expiration event that relates to the *individual* or the purpose of the use or disclosure. The statement "end of the *research* study," "none," or similar language is sufficient if the authorization is for a use or disclosure of *PHI* for *research*, including for the creation and maintenance of a *research* database or *research* repository; and
6. Signature of the *individual* and date. If the authorization is signed by a *personal representative* of the *individual*, a description of such representative's authority to act for the *individual* must also be provided.

Required Statements
In addition to the core elements, authorizations must contain at least three statements. The general topics are an *individual*'s ability to revoke the authorization in writing including exceptions to that right; whether there is a prohibition on the conditioning of *treatment*, *payment*, enrollment or eligibility for benefits on the authorization and, when there is no prohibition, the consequences for the *individual* if they refuse to sign; and the potential that information will be redisclosed by the recipient without protection if the *individual* signs the authorization. The statements required are further detailed below:

Three Statements to be Included in All Authorizations:
The statements must be adequate to place the *individual* on notice of all of the following:

1. The *individual*'s right to revoke the authorization in writing, and either:

a. A description of how the *individual* may revoke the authorization and any exceptions to that right (Please see below for details on exceptions to the right to revoke); or
b. A referral to the Notice of Privacy Practice if a description of how to revoke and the exceptions to that right are covered in that Notice of Privacy Practices;

2. The ability or inability to condition *treatment*, *payment*, enrollment or eligibility for benefits on the authorization, by stating either:
    a. The **Organization,** (or other *covered entity* if reviewing an authorization from a different entity) may not condition *treatment*, *payment*, enrollment, or eligibility for benefits on whether the *individual* signs the authorization when the prohibition on conditioning of authorizations applies (please see below for details on when this prohibition applies); or
    b. The consequences to the *individual* of a refusal to sign the authorization when the prohibition does not apply (i.e., for *research*, health plan eligibility, underwriting purposes, and risk rating determinations) - the **Organization** or the *covered entity* from whom **Organization** is accepting an authorization, can condition *treatment*, enrollment in a health plan, or eligibility for benefits on failure to obtain such authorization; and
3. The potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer be protected by *HIPAA* privacy rules.

Additional Authorization Statement Requirements for Marketing or Sale of *PHI*:
For any authorization related to the sale of *PHI* or the use or disclosure of *PHI* for marketing purposes, a fourth statement must be included for the authorization to be valid.

Additional Statement for Sale of PHI
The Privacy Rule requires that any sale of *PHI* can only be made after the *individual* has authorized such sale. An authorization form obtained to allow the sale of an *individual*'s *PHI* must include a statement that Organization will receive remuneration from a third party for the disclosure of the information. The details of the remuneration need not be detailed.

Additional Statement for Use and Disclosure of PHI for Marketing purpose:
When a) an authorization is required for marketing purposes (see Marketing section below for further details on when authorizations are not required for Marketing) *and* b) **Organization** will receive some type of remuneration from a third party for providing the *PHI*, authorizations must include a statement disclosing that remuneration is involved, but not the details of what that remuneration is.

Defective Authorizations
An authorization is not valid, and the **Organization** will not use or accept it if the document submitted has any of the following defects:

1. It is expired: the expiration date has passed, or the expiration event is known by the **Organization** to have occurred;

2. It is incomplete: the authorization has not been filled out completely, with respect to an element described by this policy, if applicable;
3. It is revoked: the authorization is known by the **Organization** to have been revoked;
4. The authorization is defective, it is an invalid compound authorization or it conditions *treatment*, *payment*, enrollment or eligibility for benefits on the authorization inappropriately or without the correct statement regarding that condition; and
5. Any material information in the authorization is known by the **Organization** to be false.

Compound Authorizations

Organization will only use and accept compound authorizations when they are acceptable under the Privacy Rule: An authorization for use or disclosure of *PHI* may not be combined with any other document to create a compound authorization, except as follows:

1. An authorization for the use or disclosure of *PHI* for a *research* study may be combined with any other type of written permission for the same or another *research* study. This exception allows combining another authorization for the use or disclosure of *PHI* for such *research* or a consent to participate in such *research* and authorization for the creation or maintenance of a *research* database or repository. If any of the authorizations included in the compound document also include a conditioning of *treatment*, *payment*, enrollment or eligibility for benefits, it must be made clear to the *individual* which parts of the compound authorization are subject to that condition and which parts are not;
2. An authorization for a use or disclosure of *psychotherapy notes* may only be combined with another authorization for a use or disclosure of *psychotherapy notes*; and
3. An authorization under this policy, other than an authorization for a use or disclosure of *psychotherapy notes*, may be combined with any other such authorization, except when the **Organization** has conditioned the provision of *treatment*, *payment*, enrollment in the health plan or eligibility for benefits on the provision of one of the authorizations. Compound authorizations that contain at least one conditioned authorization are only allowed as set forth in paragraph 1 above concerning compound *research* authorizations.

Prohibition on Conditioning of Authorizations with Exceptions

The **Organization** will not condition *treatment*, *payment*, or enrollment in a health plan, or eligibility for benefits on the provision of an authorization, except in the following circumstances allowed under the Privacy Rule:

1. The **Organization**, when acting in the capacity of health care *provider*, may condition the provision of *research*-related *treatment* on provision of an authorization for the use or disclosure of *PHI* for such *research*;
2. The **Organization,** only when acting in the capacity of a health plan, may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan *prior to* an *individual*'s enrollment in the health plan, if:
    a. The authorization sought is for the health plan's eligibility or enrollment determinations relating to the *individual*, or for its underwriting or risk rating determinations; or

b. The authorization is not for a use or disclosure of *psychotherapy notes*.

3. The **Organization** may require an authorization for release of information to a third party before providing health care that is solely for the purpose of creating *PHI* for disclosure to a third party.

Revocation of Authorizations

An *individual* may revoke an authorization at any time, provided that the revocation is in writing, and **Organization** will respect that revocation except to the extent that:

1. The **Organization** has taken action in reliance thereon; and
2. If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy, or the policy itself.

Circumstances in Which an Authorization is Specifically Required under the Privacy Rule

The Privacy rule contains special provisions related to authorizations and the sale of *PHI* in all circumstances and for the use or disclosure of Psychotherapy records, and the use or disclosure of *PHI* for marketing purposes, in most circumstances. Organization will require authorizations in all instances where it is required as further described below and in Privacy Policy 19.0: *Psychotherapy notes.*

***Psychotherapy notes*:**

Organization will utilize an Authorization for the use or disclosure of *psychotherapy notes* specific to the *psychotherapy notes* and may not combine the authorization with any other consent or authorization except for another authorization for the use or disclosure of *psychotherapy notes*.

For the details on what *psychotherapy notes* are, who may *access* them, the limited circumstances in which they can be released with an authorization, and releases that are allowed without obtaining an *individual* authorization, refer to Privacy Policy 19.0: *Psychotherapy notes* which details the appropriate *treatment* of these records.

Marketing:

Organization may use or disclose *PHI* for certain marketing purposes and for broader marketing purposes with authorization as set forth below.

Authorization to Use or Disclose *PHI* for Marketing Purposes:

1. The **Organization** shall obtain written authorization for any use or disclosure of *PHI* for marketing, except if the communication is in the form of:
    a. Face-to-face communication with the *individual*;
    b. A promotional gift of nominal value provided by the **Organization**.
    c. communications only about government or government sponsored programs; or

d. communications promoting health in general and not promoting a product or service or particular *provider*.

2. If the marketing involves the **Organization's** receiving direct or indirect remuneration from a third party, written authorization is required. If the marketing activity involves remuneration, Organization will reflect that remuneration in the authorization.

What is Marketing under the Privacy Rule?

Organization will make determinations about what activities it undertakes that fall within the Privacy Rule's definition of marketing. No *workforce member* shall engage in any activity that might be marketing before determining whether it falls within this definition to assure that any necessary authorizations are in place prior to the use or disclosure of *PHI* for which an authorization is required.

Any activity is considered "marketing "under the Privacy Rule when it is a communication about a product or service that encourages the recipients of the communication to purchase or use the product or service UNLESS it is specifically excluded from the definition. An activity can but does not have to involve remuneration to be considered marketing. If the activity is marketing and involves remuneration, Organization will reflect that remuneration in the authorization.

Determining what is Marketing
Workforce members will determine in consultation with the *Privacy Officer* whether the activity is marketing. Organization may create standard analysis for communications of the same type and content

Workforce members must go through the following set of questions until a determination on the need for an authorization is reached. Financial remuneration does not include in-kind remuneration for the purpose of this analysis and only includes monetary remunerations such as cash, checks, and wire transfers.

A. Is the communication face to face or a promotional gift of nominal value?
   If yes, no further analysis needs to be undertaken and the communication is allowed.
B. Is the communication only about government or government sponsored programs? If yes, no further analysis needs to be undertaken and the communication is allowed.
C. Is the communication promoting health in general and not promoting a product or service or particular *provider*?
   If yes, no further analysis needs to be undertaken and the communication is allowed.
D. Is the communication about a product or service that encourages the recipients of the communication to purchase or use the product or service.?
   If yes, keep *continuing to the next question until a determination is made.*
E. Is the communication a refill reminder or about a drug or biologic that is currently being prescribed for the *individual*? If no, move to the next question. If yes, also answer:

a. Is any financial remuneration being received? If not, the communication is allowed under the Privacy Rule without an authorization and **Organization** may proceed. If yes, also answer
b. If financial remuneration is being received, is it reasonably related to the Organization's cost in making the communication? If yes, no authorization is required. If no, then an authorization must be obtained prior to making the communication.

F. Is the communication for *treatment* of an *individual* by a health care *provider*, including case management or care coordination for the *individual*, or to direct or recommend alternative *treatment*s, therapies, health care *providers*, or settings of care to the *individual*?
If yes, also answer:

- Is any financial remuneration being received? If not, the communication is allowed under the Privacy Rule without an authorization and **Organization** may proceed. If yes, Organization will obtain a valid authorization reflecting remuneration prior to proceeding.

G. Does the communication describe a health-related product or service (or *payment* for such product or service) that is provided by, or included in a plan of benefits of, the *covered entity* making the communication, including communications about: health care *provider* network or health plan network participants; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefit?
If yes, also answer:

- Is any financial remuneration being received? If not, the communication is allowed under the Privacy Rule without an authorization and **Organization** may proceed. If yes, **Organization** will obtain a valid authorization reflecting remuneration prior to proceeding.

H. Is the communication related to case management or care coordination that do not fall within the definition of *treatment* and include contacting *individual*s with information about *treatment* alternatives or related functions?
If yes, also answer:

- Is any financial remuneration being received? If not, the communication is allowed under the Privacy Rule without an authorization and **Organization** may proceed. If yes, Organization will obtain a valid authorization reflecting remuneration prior to proceeding.

Sale of Protected Health Information:
Organization will obtain an authorization for all disclosures of *PHI* which are a sale of *PHI* if **Organization** engages in the sale of *PHI*. A sale of *PHI* occurs when one party remunerates another, directly or indirectly, in exchange for the second party's giving *PHI* to the first party. Remuneration can be monetary or in-kind, such as computers, services or other supplies.

When an authorization is given for sale of *PHI*, the authorization must state that the disclosure will result in remuneration.

Uses and disclosures of *PHI* for the following purposes are not considered sale of protected health information:

1. For public health purposes;
2. For *research* purposes, where the only remuneration received by a *covered entity* or *business associate* is a reasonable cost-based fee to cover the cost to prepare and transmit the *PHI* for such purposes;
3. For *treatment* and *payment* purposes;
4. For the sale, transfer, merger, or consolidation of all or part of **Organization** and for related due diligence;
5. To or by a *business associate* for activities that the *business associate* undertakes on behalf of **Organization**, or on behalf of a *business associate* in the case of a subcontractor, and the only remuneration provided is by the **Organization** to the *business associate*, or by the *business associate* to the subcontractor, for the performance of such activities;
6. Made pursuant to a request under the right of *access* standard or *accounting of disclosures* standard; and
7. For any other purpose permitted by and in accordance with the applicable requirement of the Privacy Rule, where the only remuneration received by **Organization,** or the *business associate* is a reasonable, cost-based fee to cover the cost to prepare and transmit the *PHI* for such purpose or a fee otherwise expressly permitted by other law.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.508 *Uses and Disclosures for Which an Authorization is Required*
45 CFR 501 *Definitions*

Privacy Policy 14.0 Uses and Disclosures: No Authorization or Right to Agree or Object Required

FULL POLICY LANGUAGE:

Policy Purpose:

To set forth rules regarding when **Organization** may use or disclose *individual* protected health information (*PHI*) without first having to a) obtain written authorization or b) allowing the *individual* an opportunity to agree or object. To set forth requirements for when the Organization may be required to inform the *individual* of the use or disclosure and the *individual* may agree to the use or disclosure.. To set forth the parameters for when the Organization may use and disclose *PHI* for *treatment*, *payment* and *health care operations*.

Policy Description:

Under several circumstances, the *HIPAA* Privacy Rule permits **Organization** to use or disclose *PHI* without written authorization or an opportunity to agree or object. Generally, written authorization or an opportunity to agree or object are *not* required when a use or disclosure is for *treatment*, *payment*, or healthcare operations purposes. In addition, written authorization or an opportunity to agree or object are generally *not* needed when a law *requires* that **Organization** use or disclose certain *PHI*.

Procedures:

Use and Disclosure for *Treatment*, *Payment* and *Health care operations*

Each *workforce member* should be familiar with what activities are included in *treatment*, *payment* and *health care operations* under the Privacy Rule. Also frequently referred to as TPO, it is very important for work force *members* to understand the scope of what is covered because it informs many of the day-to-day privacy and information *access* decisions they will be making concerning the use and disclosure of *PHI*. If a *workforce member* is unsure of what is included, they should review this policy and seek assistance from their supervisor or the *Privacy Officer* for clarity.

What is TPO under the Privacy Rule?

***Treatment*:**

The provision, coordination, or management of health care and related services, including the coordination or management of health care by a health care *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 health care.

***Payment*:**

Activities undertaken by a health care *provider* or health plan to obtain or provide reimbursement for the provision of health care. Activities undertaken by a health plan to obtain premiums or to determine the full extent of its coverage and benefit provision under the health plan.

Examples of *payment* activities include

- eligibility of coverage determination,
- billing,
- claims management,
- collection activities,
- medical necessity determinations,
- risk adjustments,
- utilization review including precertification, preauthorization, concurrent and retrospective review of services, and
- disclosures to consumer reporting agencies (limited to specified identifying information about the *individual*, his or her *payment* history, and identifying information about the **Organization**).

Healthcare Operations:
Any of the following activities of a *covered entity* to the extent that the activities are related to a covered function:

1. Quality assessment and improvement activities (including outcome evaluation and clinical guideline development); patient safety; population-based activities related to improving health or reducing health care costs, protocol development, case management and care coordination, contacting health care *providers* and recipients with information about *treatment* alternatives, related activities that do not include *treatment*;
2. Reviewing the competence, qualifications, performance of health care professionals, health plan performance, conducting health care training programs for students, trainees or practitioners under supervision for practice and improvement of skills; training of non-health care professionals, accreditation, certification, licensing, or credentialing;
3. Underwriting (excluding any use of genetic information), enrollment, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, ceding, securing or placing a contract for reinsurance of healthcare claim risks;
4. conducting or arranging for medical review, legal services, and auditing functions including fraud and abuse detection and compliance programs;
5. business planning and development including formulary development and administration, development or improvement of *payment* or coverage policies;
6. business management and general administrative activities of the entity which include but are not limited to:
    a. Management activities relating to implementation of and compliance with the Privacy Rule;
    b. Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
    c. Resolution of internal grievances;
    d. The sale, transfer, merger, or consolidation of all or part of the *covered entity* with another *covered entity*, or an entity that following such activity will become a *covered entity* and due diligence related to such activity; and
    e. Consistent with the applicable requirements of creating de-identified health information or a *limited data set* and *fundraising* for the benefit of the *covered entity*.

Organization May Seek Consent for TPO Uses and Disclosures
While Organization may request an *individual*'s consent for the use of *PHI* for *treatment*, *payment* and *health care operations*, it may not condition the provision of services or insurance on the *individual* granting consent. **Organization** does not *require* consent for the use of *PHI* for *treatment*, *payment* and operations. The **Organization** may make exception for this when such consent is specifically required by other legal requirements like in cases for *research* consents. Any consent provided by an *individual* for **Organization's** use of *PHI* for TPO purposes will not

be treated as an authorization and the consent does not permit otherwise prohibited sharing of *PHI*.

If an *individual* is asked for consent but declines to provide it, **Organization** may still utilize their *PHI* for TPO purposes unless otherwise prohibited by another provision of the Privacy Rule.

Organization's Uses and Disclosures for *Treatment Payment* and *Health care operations*
Organization permits use or disclosure of protected health information for *treatment*, *payment*, or *health care operations* as set forth below, provided that such use or disclosure is consistent with other applicable requirements of the Privacy Rule.

Organization permits work force *members* to use or disclose protected health information

1. for Organization's own *treatment*, *payment*, or *health care operations*.
2. for *treatment* activities of a health care *provider*.
3. to another *covered entity* or a health care *provider* for the *payment* activities of the entity that receives the information.
4. to another *covered entity* for *health care operations* activities of the entity that receives the information, if each entity either has or had a relationship with the *individual* who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:
    a. For a purpose listed in paragraph (1) or (2) of the definition of *health care operations* above; or
    b. For the purpose of health care fraud and abuse detection or compliance; and
5. (If the Organization is participating in an organized health care arrangement), *workforce members* may disclose protected health information about an *individual* to other participants in the same organized health care arrangement for the *health care operations* activities of the organized health care arrangement.

<u>Other Uses and Disclosures Which Do Not Require Authorizations or Opportunities to Agree or Object prior to Organization's Use or Disclosure of *PHI*</u>

For each of the following topics on use and disclosure listed below, Organization *workforce members* will use and disclose *PHI* without the need for obtaining a valid authorization or providing an *individual* the opportunity to agree or object following the parameters detailed for each topic in the sections below and in the separate policies noted next to the topics of Worker's Compensation and Judicial and Administrative Proceedings.

Uses and Disclosures Required by law.
Uses and Disclosures for Public Health Activities:
Disclosures About Victims of Abuse, Neglect, or Domestic Violence
Uses and Disclosures for Health Oversight Activities
Uses and Disclosures for Judicial and Administrative Proceedings (See Privacy Policy 22.0)
Uses and Disclosures for Law Enforcement Purposes

Uses and Disclosures About Decedents:
Uses and Disclosures for Cadaveric Organ, Eye or Tissue donation purposes
Uses and Disclosures for *Research* Purposes:
Uses and Disclosures to Avert a Serious Threat to Health or Safety:
Uses and Disclosures for Specialized Government Functions
Uses and Disclosures for Workers Compensation (See Privacy Policy 24.0)
Permitted Disclosures by Whistleblower
Permitted Disclosures by *Workforce* Member Crime Victims:
Permitted Disclosures Military and Veterans Activities

Uses and Disclosures Required by Law:

1. **Organization** will use or disclose *PHI* to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.
2. **Organization** will follow the specific *HIPAA* parameters for disclosure related to:
    a. Disclosures about victims of abuse, neglect, or domestic violence;
    b. Disclosures for judicial and administrative proceedings; and
    c. Victims of a crime.
    These parameters are detailed below in the sections dealing with each of these topics.

Uses and Disclosures for Public Health Activities:

The **Organization** may disclose *PHI* related to public health activities to:

1. A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including but not limited to, the mandatory reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority; and
2. A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.
3. A person subject to the jurisdiction of the Food and Drug Administration ("FDA") with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety, or effectiveness of such FDA-regulated product or activity. Such purposes include:
    a. To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;
    b. To track FDA-regulated products;
    c. To enable product recalls, repairs, replacement, or lookback (including locating and notifying *individual*s who have received products that have been recalled, withdrawn, or are the subject of lookback); or

    d. To conduct post-marketing surveillance.
4. A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if **Organization** or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.
5. An employer, about an *individual* who is a *member* of the *workforce* of the employer, if:
    a. **Organization** is the ***Workforce member's*** health care *provider* who provides health care to the *individual* at the request of the employer:
        i. To conduct an evaluation relating to medical surveillance of the workplace; or
        ii. To evaluate whether the *individual* has a work-related illness or injury.
    b. The *PHI* that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;
    c. The employer needs such findings in order to comply with its obligations under OSHA, MSHA, or under State law having a similar purpose to record such illness or injury, or to carry out responsibilities for workplace medical surveillance; or
    d. The covered health care *provider* provides written notice to the *individual* that *PHI* relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:
        i. By giving a copy of the notice to the *individual* at the time the health care is provided; or
        ii. If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.
6. A school, about an *individual* who is a student or prospective student at the school, if:
    a. The *PHI* that is disclosed is limited to proof of immunization;
    b. The school is required by state or other law to have such proof of immunization prior to admitting the *individual*; and
    c. **Organization** obtains and documents the agreement to the disclosure from either:
        i. A parent, guardian, or other person acting *in loco parentis* of the *individual*, if the *individual* is an unemancipated minor; or
        ii. The *individual*, if the *individual* is an adult or emancipated minor.

If Organization is, or ever becomes a public health authority, *workforce members* may use *PHI* in all cases where it is permitted to disclose such information for public health activities in paragraphs 1 and 2 above.

Disclosures About Victims of Abuse, Neglect, or Domestic Violence:

1. The **Organization** may disclose *PHI* about an *individual* whom the **Organization** reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency authorized by law to receive reports of such abuse, neglect, or domestic violence:

a. To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;
b. If the *individual* agrees to the disclosure; or
c. To the extent the disclosure is expressly authorized by statute or regulation, and:
    i. The **Organization**, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the *individual* or other potential victims; or
    ii. If the *individual* is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the *PHI* for which disclosure is sought 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.

2. When a disclosure about victims of abuse, neglect, or domestic violence is made, the **Organization** must promptly inform the *individual* that such a report has been or will be made, except if:
    a. The **Organization**, in the exercise of professional judgment, believes that informing the *individual* would place the *individual* at risk of serious harm; or
    b. The **Organization** would be informing a *personal representative* and the **Organization** 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 **Organization**, in the exercise of professional judgment.

Uses and Disclosures for Health Oversight Activities:

1. The **Organization** may disclose *PHI* to a health oversight agency for oversight activities authorized by law, including: audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:
    a. The healthcare system;
    b. Government benefits programs for which health information is relevant to beneficiary eligibility;
    c. Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
    d. Entities subject to civil rights laws for which health information is necessary for determining compliance.
2. "Health oversight activities," for purposes of (1) above, do not include an investigation or other activity in which the *individual* is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:
    a. The receipt of health care;
    b. A claim for public benefits related to health; or
    c. Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

3. Notwithstanding (2) immediately above, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of this policy.
4. If the **Organization** also is a health oversight agency, the **Organization** may use *PHI* for health oversight activities as permitted by this policy.

Use and Disclosure for Law Enforcement Purposes
Organization will follow these requirements for the release of *PHI* for law enforcement purposes via court orders, court-ordered warrant, a judicial or grand jury subpoena, or summons including considerations for administrative and civil investigative demands.

Standard: Disclosures for law enforcement purposes. Organization may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs 1 through 6 below are met, as applicable.

1. ***Permitted disclosures: Pursuant to process and as otherwise required by law.*** A *covered entity* may disclose protected health information:
    a. As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject disclosure of abuse, neglect or domestic violence or if the victim agrees to the disclosure of this section; or
    b. In compliance with and as limited by the relevant requirements of:
        i. A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
        ii. A grand jury subpoena; or
        iii. An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:
            1. The information sought is relevant and material to a legitimate law enforcement inquiry;
            2. The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
            3. *De-identified information* could not reasonably be used. See Also Privacy Policy 22.0: *Uses and Disclosures: Response to Judicial and Administrative Proceedings*.
2. ***Permitted disclosures: Limited information for identification and location purposes.*** Except for disclosures required by law as permitted by paragraph 1 above. **Organization** may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:
    a. **Organization** will disclose only the following information:
        i. Name and address;

ii. Date and place of birth;
iii. Social security number;
iv. ABO blood type and rh factor;
v. Type of injury;
vi. Date and time of *treatment*;
vii. Date and time of death, if applicable; and
viii. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.
ix. Except as permitted by paragraph 2(i)above, the *covered entity* may not disclose for the purposes of identification or location under this paragraph any protected health information related to the *individual*'s DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

3. ***Permitted disclosure: Victims of a crime.*** Except for disclosures required by law as permitted by paragraph 1 above, **Organization** may disclose protected health information in response to a law enforcement official's request for such information about an *individual* who is or is suspected to be a victim of a crime, other than disclosures that are subject to disclosures for public health activities or disclosures regarding victims of abuse, neglect or domestic violence, if:
    a. The *individual* agrees to the disclosure; or
    b. The *covered entity* is unable to obtain the *individual*'s agreement because of incapacity or other emergency circumstance, provided that:
        i. The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
        ii. The law enforcement official represents that immediate law 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; and
        iii. The disclosure is in the best interests of the *individual* as determined by the Organization, in the exercise of professional judgment.

Uses and Disclosures About Decedents:

1. Coroners and medical examiners: The **Organization** may disclose *PHI* to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A *Covered entity* that also performs the duties of a coroner or medical examiner may use *PHI* for the purposes described in this paragraph.
2. The **Organization** may disclose *PHI* to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If it is necessary for funeral directors to carry out their duties, the **Organization** may disclose the *PHI* prior to, and in reasonable anticipation of, the *individual*'s death.

3. The **Organization** may use or disclose *PHI* to organ procurement Organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation.

Uses and Disclosures About Decedents:

1. Coroners and medical examiners: The **Organization** may disclose *PHI* to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A *Covered entity* that also performs the duties of a coroner or medical examiner may use *PHI* for the purposes described in this paragraph.
2. The **Organization** may disclose *PHI* to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If it is necessary for funeral directors to carry out their duties, the **Organization** may disclose the *PHI* prior to, and in reasonable anticipation of, the *individual*'s death.
3. The **Organization** may use or disclose *PHI* to organ procurement Organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation of facilitating organ, eye, or tissue donation and transplantation.

Uses and disclosures for cadaveric organ, eye or tissue donation purpose

Organization may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

Uses and Disclosures for *Research* Purposes:

1. The **Organization** may use or disclose *PHI* for *research*, regardless of the source of funding of the *research*, provided that:
    a. The **Organization** obtains documentation that an alteration to or waiver, in whole or in part, of the *individual* authorization for use or disclosure of *PHI* has been approved by either:
        i. An *Institutional Review Board* (*IRB*); or
        ii. A privacy board that:
            a. Has *members* with varying backgrounds and appropriate professional competency as necessary to review the effect of the *research* protocol on the *individual*'s privacy rights and related interests;
            b. Includes at least one *member* who is not affiliated with the **Organization**, not affiliated with any entity conducting or sponsoring the *research*, and not related to any person who is affiliated with any of such entities; and

c. Does not have any *member* participating in a review of any project in which the *member* has a conflict of interest.

i. Reviews preparatory to *research*. The **Organization** obtains from the *research*er representations that:

i. Use or disclosure is sought solely to review *PHI* as necessary to prepare a *research* protocol or for similar purposes preparatory to *research*;

ii. No *PHI* is to be removed from the **Organization** by the *research*er in the course of the review; and

iii. The *PHI* for which use or *access* is sought is necessary for the *research* purposes.

b. (*Research* on decedent's information). The **Organization** obtains from the *research*er:

i. Representation that the use or disclosure sought is solely for *research* on the *PHI* of decedents;

ii. Documentation, at the request of the **Organization**, of the death of such *individual*s; and

iii. Representation that the *PHI* for which use or disclosure is sought is necessary for the *research* purposes.

2. Documentation of Waiver Approval

For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, the documentation must include all of the following:

i. A statement identifying the *IRB* or privacy board and the date on which the alteration or waiver of authorization was approved;

ii. A statement that the *IRB* or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

1. The use or disclosure of *PHI* involves no more than a minimal risk to the privacy of *individual*s based on, at least, the presence of the following elements:

a. An adequate plan to protect the identifiers that lead to *individuals* from improper use and disclosure;

b. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the *research*, unless there is a health or *research* justification for retaining the identifiers or such retention is otherwise required by law; and

c. Adequate written assurances that the *PHI* will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the *research* study, or for other *research* for which the use or disclosure of *PHI* is needed;

3. The *research* could not practically be conducted without the waiver or alteration; and

i. The *research* could not practically be conducted without *access* to and use of the *PHI*;

b. A brief description of the *PHI* for which use or *access* has been determined to be necessary by the *IRB* or privacy board, as determined pursuant to the above paragraph;
c. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:
    i. The Internal Review Board must follow the requirements of the *HIPAA* Rules, including the normal review procedures or the expedited review procedures;
    ii. The Privacy Board must review the proposed *research* at a convened meeting at which a majority of the privacy board *members* are present, including at least one *member* who satisfies the *Privacy Officer* or Compliance Officer title, and the alteration or waiver of authorization must be approved by the majority of the privacy board *members* present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with the below paragraph; and
    iii. A Privacy Board may use an expedited review procedure if the *research* involves no more than minimal risk to the privacy of the *individual*s who are the subject of the *PHI* for which use or disclosure is being sought. If the Privacy Board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the Privacy Board, or by one or more *members* of the Privacy Board as designated by the chair; and
d. The documentation of the alteration or waiver of authorization must be signed by the chair or other *member*, as designated by the chair of the *IRB* or the privacy board, as applicable.

(iii) ***Protected health information needed.*** A brief description of the protected health information for which use or *access* has been determined to be necessary by the institutional review board or privacy board, pursuant to paragraph (i)(2)(ii)(C) of this section;

(iv) ***Review and approval procedures.*** A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:

(A) An *IRB* must follow the requirements of the Common Rule, including the normal review procedures or the expedited review.
(B) A privacy board must review the proposed *research* at convened meetings at which a majority of the privacy board *members* is not affiliated with the **Organization**, and the alteration or waiver of authorization must be approved by the majority of the privacy board *members* present at the meeting, unless the privacy board elects to use an appropriate expedited review procedure;
(C) A privacy board may use an expedited review procedure if the *research* involves no more than minimal risk to the privacy of the *individual*s who are the subject of the protected health information for which use or disclosure is being

sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more *members* of the privacy board as designated by the chair; and

(v) ***Required signature.*** The documentation of the alteration or waiver of authorization must be signed by the chair or other *member*, as designated by the chair, of the *IRB* or the privacy board, as applicable.

Uses and Disclosures to Avert a Serious Threat to Health or Safety:

1. The **Organization** may, consistent with applicable law and standards of ethical conduct, use or disclose *PHI* if the **Organization**, in good faith, believes that the use or disclosure:
    a. Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public;
    b. Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat;
    c. Is necessary for law enforcement authorities to identify or apprehend an *individual*:
        i. Because of a statement by an *individual* admitting participation in a violent crime that the **Organization** reasonably believes may have caused serious physical harm to the victim; and
        ii. Where it appears from all the circumstances that the *individual* has escaped from a correctional institution or from lawful custody.
2. A use or disclosure pursuant to this policy may not be made if the information described is learned by the **Organization:**
    a. Over the course of *treatment*, counseling, or therapy to affect the propensity to commit the criminal conduct that is the basis for the disclosure under this policy; or
    b. Through a request by the *individual* to initiate or to be referred for *treatment*, counseling, or therapy described in the above paragraph;
3. A disclosure made pursuant to (1)(a)(i) above shall contain a statement that *PHI* is necessary for law enforcement to apprehend or identify an *individual* because of a statement by an *individual* admitting participation in a violent crime that the *covered entity* reasonably believes may have caused serious harm to the victim, AND the following information: name and address; date and place of birth; social security number; ABO blood type and rhesus factor; type of injury; date and time of *treatment*; date and time of death, if applicable; and a description of distinguishing physical characteristics, such as height, weight, gender, hair, and eye color.
4. The **Organization**, when using or disclosing *PHI*, is presumed to have acted in good faith if the belief is based upon the **Organization's** actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

Uses and Disclosures for Specialized Government Functions:
Organization may use and disclose an *individual*'s protected health information (*PHI*) without an *individual*'s written authorization for the following specialized government functions:

- Military and veterans' activities
- National security and intelligence activities
- Protective services for the President and others
- Medical suitability determinations
- Correctional institutions and other law enforcement custodial situations

Under the Privacy Rule "*whistleblower* exception," *workforce members* and their *business associates*, have the right to disclose *PHI* if they believe in good faith that another *workforce member* or *business associate* has engaged in conduct that is unlawful or otherwise violates professional standards *Workforce members* may also report that services or conditions provided by a *member* of the *workforce*, a department, or a *business associate*, are endangering one or more participants, workers, or the public.

Permitted Disclosures by Whistleblower:

1. **Organization's** *workforce members* and *business associates* may make *whistleblower* disclosures of an *individual*'s *PHI* without the *individual*'s written authorization.
2. **Organization** will not impose any sanctions upon and will not take any intimidating or retaliatory actions against *members* of **Organization's** *workforce* and **Organization's** *Business associates* who make Whistleblower Disclosures related to **Organization's** handling of *PHI* and compliance with *HIPAA*.
3. **Organization** does not violate *HIPAA* if a *member* of its *workforce* or its *business associate* makes a *whistleblower* disclosure in compliance with the requirements of this policy.
4. Under the *HIPAA whistleblower* exception, **Organization** is not considered to have violated the *HIPAA* Privacy Rule if a *member* of its *workforce* or a *business associate* discloses protected health information (*PHI*), provided that the requirements of (a), (b), and (c) below, are met:
    a. The *workforce member* believes, in good faith, that:
        i. The **Organization** has engaged in unlawful conduct; or
        ii. The **Organization** has engaged in conduct that otherwise violates professional or clinical standards; or
        iii. The care, services, or conditions provided by the **Organization** potentially endanger patients, workers, or the public.
    b. The *PHI* "*whistleblower*" disclosures listed in (1) through (3) above are made to:
        i. An appropriate healthcare accreditation Organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the **Organization**; **or**

ii. A health oversight agency or public health authority that has the authority to investigate or oversee the relevant conduct or conditions of the **Organization**; **or**

iii. An attorney retained by or on behalf of the *workforce member* or *business associate* for the purpose of determining the legal options of the *workforce member* or *business associate* with regard to the conduct alleged to be improper.

c. Limitation on Disclosures: Disclosures can only be made if the ***Workforce member***

has a good faith belief that improper conduct has taken place. Broadly speaking, "good faith belief" means a belief with a reasonable basis in fact. Generally, a person is not acting in good faith if he or she knows or should have known that he or she is making a malicious, false, or frivolous allegation or complaint.

Permitted Disclosures by *Workforce* Member Crime Victims:

1. A *workforce member* who is a victim of a criminal act has the right to disclose *PHI* to law enforcement officials. Such a disclosure will not constitute a violation of the Privacy Rule by the **Organization** if the following conditions apply:
    a. The *PHI* disclosed is about the suspected perpetrator of the criminal act; and
    b. The *PHI* disclosed is limited to the following information:
        i. Name and address
        ii. Date and place of birth
        iii. Social Security Number
        iv. ABO blood type and rh (rhesus) factor
        v. Type of injury
        vi. Date and time of *treatment*
        vii. Date and time of death, if applicable; and
        viii. A description of distinguishing physical characteristics.
2. If a *workforce member* considers himself or herself a *workforce* crime victim, he/she should immediately notify the *HIPAA Privacy Officer*, who shall advise the *workforce member* as to what *PHI* (see paragraph (1)) may be disclosed to law enforcement.

Permitted Disclosures Military and Veterans Activities.

1. Armed Forces Personnel: **Organization** may disclose to military authorities the *PHI* of *individual*s who are *members* of the armed forces for purposes that appropriate military command authorities have deemed necessary to ensure proper execution of the military mission.
2. Before the military authority may seek the information, the military authority must publish a notice in the Federal Register that sets forth both the name of the appropriate military command authorities, **and** the purposes for which the *PHI* may be used or disclosed.
3. Foreign Military Personnel: **Organization** may use or disclose to the appropriate military authority the *PHI* of *individual*s who are foreign military personnel for the same

purposes for which **Organization** may use or disclose *PHI* regarding Armed Forces Personnel as described above.

4. National Security and Intelligence Activities: **Organization** may disclose *PHI* to authorized federal officials as necessary to conduct lawful intelligence, counterintelligence, and other national security activities authorized by the National Security Act (50 U.S.C. § 401, et. seq.) and implementing authority (i.e., Executive Order 12333).
5. Protective Services for the President and Others: **Organization** may disclose an *individual*'s *PHI* to authorized federal officials for the provision of protective services to the President of the United States or other persons authorized by 18 U.S.C. § 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. § 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. §§ 871 (Threats Against the President and Successors to the Presidency) and 879 (Threats Against Former Presidents and Others).
6. Correctional Institutions and Other Law Enforcement Custodial Situations: **Organization** may disclose an *individual*'s *PHI* to a correctional institution or a law enforcement official who has lawful custody of an inmate or other individual if the correctional institution or law enforcement official represents that such *PHI* is necessary for:
7. The provision of healthcare to the *individual*;
8. The health and safety of such *individual* or another inmate;
9. The health and safety of the officers, ***Workforce members***, or others at the correctional institution;
10. The health and safety of such *individual* and officers or other persons responsible for the transporting of inmates or their transfer from one institutional facility or setting to another; or
11. The administration and maintenance of safety, security, and good order of the correctional institution;

The *PHI* of an *individual* who has been released on parole, probation, supervised release, or who is otherwise no longer in lawful custody, may not be used or disclosed.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.501 *Definitions: Healthcare Operations*
45 CFR 164.512 *Uses and Disclosures for which an Authorization or Opportunity to Agree or Object is Not Required*
45 CFR 164.506 *Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations*

Privacy Policy 15.0. Individual Right: Access to Protected Health Information

FULL POLICY LANGUAGE:

Policy Purpose:

It is the policy of the **Organization** to honor an *individual*'s right to *access*, inspect, and obtain a copy of their *PHI* contained in the *designated record set* and to charge only allowable fees for such *access*.

Policy Description:

This policy describes **Organization's** responsibility for providing *access* to a *designated record set* to *individual*s for as long as the record is maintained and the procedures for ensuring *individual*s' timely rights to *access*, inspect and copy their protected health information and seek review of some denials of *access*. Additionally, the policy establishes the requirements for determining and charging reasonable fees related to *access* requests by *individual*s.

Procedures:

Accessing and Inspecting *PHI*: Timing and Process

1. An *individual* must make a request to a *member* of the *workforce* to *access* and inspect their *PHI*. Whenever possible, this request shall be made in writing and documented on either an "Authorization for Disclosure" form or in the notes of the *individual*'s health record.
2. The *workforce member* who receives the request should direct it to the *individual* designated to handle such requests. If no such person is available and the *workforce member* is unsure of whether *access* is appropriate, they should contact their supervisor or the *Privacy Officer* to help make that determination prior to allowing or denying *access*.
3. When *access* is granted, the **Organization** will provide *access* to the requested *PHI* and furnish a copy if requested within a reasonable time but no later than 30 days from the date of the request unless the Organization is not able to provide *access* within 30 days. See below for the requirements on the form and fees for copies.
4. Where it cannot provide *access* within the 30-day time limit, before the 30 days expire, Organization will provide the *individual* a written notice of the reasons for the delay and include a date when *access* will be available. Organization will respond to all requests for *access* within 60 days of the *individual*'s request. A second extension beyond 60 days is not available.
5. The **Organization** must document and retain the *Designated record set*s containing the *PHI* that is subject to *access*. The **Organization** must document and retain the titles of persons or offices responsible for receiving and processing requests for *access*. These records must be maintained for a minimum of six years form the date of creation or the date it was last in effect.

When *Access*, Inspection and/or Copy Request is Granted:

1. *Individual* and the **Organization** will arrange a mutually convenient time and place for the *individual* to inspect and/or obtain a copy of the requested *PHI* within the

designated record set. Inspection and/or copying will be carried out on site at the **Organization** with staff assistance if necessary.

2. The patient may choose to inspect the *PHI*, copy it, or both, in the form or format requested. If the *PHI* is not readily producible in the requested form or format, the **Organization** must provide the patient with a readable hard copy form, or other form or format as agreed to by the **Organization** and the *individual*.
    a. If the *individual* chooses to receive a copy of the *PHI*, the **Organization** may offer to provide copying services. The patient may request that this copy be mailed.
    b. If the *individual* chooses to copy their own information, the **Organization** may supervise the process to ensure that the integrity of the patient record is maintained.
3. Whenever the *PHI* in the *designated record set* is maintained electronically, if the *individual* requests an electronic copy, **Organization** will provide *access* in the electronic form and format requested unless it is not readily producible that way. If it is not readily producible in the requested format, **Organization** and the *individual* will agree to a different readable electronic format for production.
4. Upon prior approval by the patient, the **Organization** may provide a summary of the requested *PHI* and charge an agreed upon fee (must not exceed the fees allowed – see fee section below).
5. If, upon inspection of the *PHI*, the patient believes the *PHI* is inaccurate or incomplete, the patient has the right to request an *amendment* to the *PHI*. The **Organization** shall process requests for *amendment* as outlined in Privacy Policy 17.0: *Individual Right: Request Amendment to Designated record set*.

Fees

Organization may charge a reasonable cost-based fee for the production of copies (including electronic copies) or a summary of *PHI* pursuant to the request of an *individual* (or their *personal representative*) for their own personal use. **Organization** may decide to waive such fees. For electronic record requests, **Organization** may decide to charge a flat fee in lieu of a cost-based fee.

<u>Such fees may only include the actual or average cost of:</u>

1. Labor for copying the protected health information, whether in paper or electronic form;
2. Supplies for creating the paper copy if paper is requested;
3. Electronic media if the *individual* requests an electronic copy be provided on portable media;
4. Postage when the *individual* requests that the phi or summary be mailed; and
5. Preparation of a Summary or Explanation of the *PHI* when the *individual* was informed in advance and agreed to the stated fee.

Organization, unless charging the flat fee for electronic records, elects to utilize the actual cost associated with the requests rather than determining average or per page costs in determining fees**.**

Such fees may *not* include:

1. costs associated with verification; documentation; searching for, handling, or retrieving the *PHI*; processing the request; maintaining systems; or recouping capital for data *access*, storage, or infrastructure, even if such costs are authorized by State law.
2. Fees established by state law where such fees are in excess of that allowed under *HIPAA*. State laws typically permit *providers* to charge a per-page copy fee, of up to a certain dollar value, or to charge a flat fee of up to a certain amount for the entire *medical record*. These fees are untethered to the actual costs of reproduction and can be in excess of that allowed under *HIPAA*.
3. Costs for providing, releasing, or delivering *medical record*s or copies of *medical record*s, where the request is for the purpose of supporting the application, claim, or appeal for any government benefit or program requested by the relevant government entity or at the *individual*'s request.

Flat Fee

Organization, in its discretion, may charge *individual*s a flat fee for all requests for electronic copies of *PHI* maintained electronically, provided the fee does not exceed $6.50, inclusive of all labor, supplies, and any applicable postage. **Organization** may charge this fee in lieu of going through the process of calculating actual or average allowable costs for requests for electronic copies of *PHI*.

***Access*, Inspection, and/or Copy Request is Denied in Whole or in Part:**

The **Organization** will deny *access* to any *PHI* without the opportunity for review if it contains:

1. *Psychotherapy notes* (See Privacy Policy 19.0: *Psychotherapy notes* for further details); or
2. Information compiled in reasonable anticipation of, or for use in, civil, criminal, or administrative action or proceeding.

If any part of the *designated record set* is separate from *psychotherapy notes* or information compiled in anticipation of legal proceedings, Organization shall allow *access* to that part of the record.

The Organization May Deny *Access* without Providing the *Individual* an Opportunity for Review, in the Following Circumstances:

1. When **Organization** is acting under the direction of a Correctional Institution and may deny an inmate's request if it were to jeopardize the health, safety, security, custody, or rehabilitation of the *individual*, other inmates, or any other person at the correctional institution.
2. When *PHI* created in the course of *research* that is still in progress, provided the *individual* has agreed to the denial of *access* when consenting to participating in the *research* that includes *treatment*, and the covered health care *provider* had informed the *individual* that the right of *access* would be reinstated upon completion of the *research*.

3. When *PHI* in the *designated record set* was obtained under promise of confidentiality from someone other than a healthcare *provider* and giving *access* would reveal the source of the information.
4. An *individual*'s *access* to *PHI* that is contained in records that are subject to the Privacy Act (also known as the Freedom of Information Act) may be denied, if the denial of *access* under the Privacy Act would meet the requirements of that law.

The Organization May Deny *Access* but will Provide the Opportunity for Review of Denials in the following Circumstances:

1. When a licensed healthcare professional (exercising their professional judgment) has determined that the *access* requested is reasonably likely to endanger the life or physical safety of the *individual* or another person.
2. When the *PHI* makes reference to another person (unless that person is a healthcare *provider*) and a licensed healthcare professional has determined in exercise of professional judgment, that the *access* requested is reasonably likely to cause substantial harm to the person.
3. When request for *access* is made by a *personal representative* of an *individual* and a licensed healthcare professional has determined in exercise of professional judgment that providing *access* to that representative can reasonably be expected to cause substantial harm to the *individual* or another person.

Denials of *Access*: Timing, form and Review:

If the **Organization** denies *access* in whole or in part in any of the circumstances described above, the following requirements will apply to the denial:

Making Other information Accessible: The Organization will give the *individual access* to the protected health information that is not excluded under the denial to the extent that it is possible to separate the information for which the **Organization** has a basis for denial.

Denials will be in writing:
The **Organization** must provide a written denial in plain language to the *individual*. The denial will contain the following elements:

1. The basis for the denial;
2. A statement of the *individual*'s review rights for reviewable denials; and
3. A description of how the *individual* may complain to the **Organization** or to the Secretary of Health and Human Services (*HHS*) including at a minimum the title and telephone number of the *individual* designated to handle complaints for the **Organization**.

Other Responsibilities When *Access* is Denied:

1. If *access* is denied because the **Organization** does not maintain the *PHI* that is the subject of the request, and the **Organization** knows where that *PHI* is maintained, the **Organization** must inform the *individual* where to direct the request for *access*.

2. If *access* is denied under a situation where that denial may be reviewed, an *individual* has the right to have the denial reviewed by a licensed healthcare professional who is designated by the **Organization** to act as a reviewing official. Organization will designate a licensed professional to review the original *access* decision. The reviewing professional must be someone who did not participate in the original decision to deny *access*.
3. The patient must initiate the review of a denial by making a request for review to the **Organization**. If the patient has requested a review, the **Organization** must provide or deny *access* in accordance with the determination of the reviewing professional, who will make the determination within a reasonable period of time.
4. The **Organization** will promptly provide written notice to the *individual* of the determination of the reviewing professional and also act promptly on the reviewer's decision if they have granted *access*.

RELEVANT *HIPAA* REGULATIONS:

45 CFR 164.524 *Access of Individuals to Protected Health Information*

Privacy Policy 16.0 Individual Right: to Request Restrictions and Alternate Confidential Communications

FULL POLICY LANGUAGE:

Policy Purpose:

This policy covers how **Organization** must assess and when it will honor *individuals*' requests to restrict how and when their *PHI* is used or disclosed, and requests for communication of *PHI* by alternative means or at an alternate location.

Policy Description:

Organization permits an *individual* to request restrictions of uses and disclosures for *treatment*, *payment*, healthcare operations and disclosures to family *members*, relatives, close friends or others identified by the *individual* for involvement in the *individual*'s care and notifications and must agree to restrictions in some circumstances involving *payment*. All granted restrictions must be fully documented for six years and adhered to if agreed except in emergency circumstances or as otherwise required by law.

Organization may also terminate restrictions previously agreed to if (1) the *individual* agrees to or requests the termination in writing, (2) the *individual* orally agrees to the termination and the oral agreement is documented, or (3) a *Covered entity* informs the *individual* it is terminating an agreement to a restriction, (under circumstance 3, termination is only effective with respect to *PHI* created or received after it has informed the *individual*).

Organization, when considering the request for restriction, may consider its own need for *access* to *PHI* for *treatment* purposes.

Organization will also honor an *individual*'s right to receive confidential communications at alternative locations or by alternative means from a health plan when an *individual* would be endangered or from a *provider* where the request is reasonable. A *Covered entity provider* may require that the request meet the following criteria: (1) be reasonable with respect to the administrative burden, (2) be in writing, (3) specify an alternative address or other method of contact, and, where relevant, provides information on how *payment*s should be handled.

Procedures:

Response to Request for Restriction:

1. Organization will notify *individual*s of the right to request restrictions on the use and disclosure of *PHI* and that the request needs to be in writing in **Organization's** Notice of Privacy Practices.
2. The *Privacy Officer* will manage requests for restrictions. All documentation associated with the request shall be placed in the *individual*'s *medical record*.
3. The Organization will provide an *individual* with a *Request to Restrict Use and Disclosure of Protected Health Information* form ("Request to Restrict" form) if an *individual* asks to make a restriction.
4. The *individual* must complete and sign the form. The *Privacy Officer* and/or his or her designee may assist the *individual* in completing the form, if necessary.
5. Once the request has been completed, the *Privacy Officer* will review it, in consultation with other **Organization** staff, to determine the feasibility of the request.
6. Organization will agree to all requests related to restrictions about communicating *PHI* to a health plan when the following criteria are met:
    a. The disclosure is for the purpose of carrying out *payment* or *health care operations* and is not required by law; *and*
    b. The protected health information pertains solely to a health care item or service for which the *individual*, or a person (other than the health plan) on behalf of the *individual*, has paid the **Organization** in full.
7. Whether requests are allowed or denied, the *Privacy Officer* will provide a written response to the *individual* and place a copy in their *medical record*.

Accepted Requests for Restrictions:

1. **Organization** will abide by the terms of any accepted restrictions with the following exceptions:
    a. **Organization** may use the restricted *PHI*, or may disclose such information to a healthcare *provider*, *if* (1) the *individual* is in need of emergency *treatment*, **and** (2) the restricted *PHI* is needed to provide that *treatment*. In this instance, **Organization** will release the *PHI*, but shall ask the emergency *treatment provider* to not further disclose or use the *PHI*.

b. **Organization** may disclose the information to the patient who requested the restriction.
c. **Organization** may use and disclose the restricted *PHI* when legally required to do so under the *HIPAA* Privacy Rule.

2. Upon accepting the restriction, the *Privacy Officer* will notify appropriate staff of the restriction.
3. The *Privacy Officer* will document the restriction on the Request to Restrict form, provide the patient with a copy, and maintain the original in the patient's *medical record*. This notation on the form can suffice for communicating the decision.

Termination of Restriction with *Individual*'s Agreement:

1. **Organization** may terminate the accepted restriction if the *individual* agrees to such termination in writing, **or** the *individual* agrees to the termination orally, and such oral agreement is documented by **Organization**.
2. **Organization** will notify appropriate staff of such termination. The *Privacy Officer* shall document the *individual*'s agreement to the termination on the Request to Restrict form, provide the *individual* with a copy, and maintain the documentation in the *individual*'s record.
3. Termination of a restriction with the *individual*'s agreement is effective for all *PHI* created, maintained or received by **Organization**.

Termination of Restriction Without *Individual*'s Agreement:

1. **Organization** may terminate the restriction without the *individual*'s agreement if the **Organization** informs the patient that the restriction is being terminated.
2. Such termination will only be effective with respect to *PHI* created or received after **Organization** has informed the *individual* that it is terminating the restriction. The **Organization** must continue to abide by the restriction with respect to all *PHI* created or received before it informed the *individual* of the restriction.
3. If **Organization** informs the *individual* by mail that it is terminating the restriction, **Organization** will send it via certified mail, return receipt requested. **Organization** will maintain a copy of the notification and the return receipt. **Organization** may only terminate the restriction upon confirmation that the *individual* has received the notification.
4. If **Organization** informs the *individual* in person that it is terminating the restriction, **Organization** will ensure that the *individual* signs and dates the notification of termination. **Organization** may alternatively document that the *individual* was notified on the *Request to Restrict* form.
5. If **Organization** informs the *individual* by telephone of the termination of the restriction, the **Organization** shall document this action and will also send the *individual* a letter via certified mail, return receipt requested. **Organization** may deem such termination to be effective as of the date it informs the resident by telephone.

Confidential Communication by Alternative Means or at Alternate Location

*Individual*s may request communication of *PHI* by alternative means or at an alternate location. **Organization** will review and respond to such requests in accordance with the below procedures.

Response to Requests for Alternative Means of Communication:

1. Patients shall be notified of the right to request communication by alternative means or at alternative locations in **Organization's** Notice of Privacy Practices. See Privacy Policy 10; *Notice of Privacy Practices*.
2. **Organization's** *Privacy Officer* shall oversee and manage requests to receive communications by alternative means.
3. **Organization** requires *individual*s make a written request for communication by alternative means or at alternate location.
4. When an *individual* inquires about the right to request the **Organization** communicate with him or her, or his or her *personal representative*, by some alternate means, **Organization** shall provide them with a *Request for Communications by Alternative Means* ("Request for Communications") form. No request shall be evaluated until the request form has been completed and signed by the *individual* or their *personal representative*.
5. **Organization,** *if acting as a health plan*, may require that requests be accompanied by a statement that disclosure of *PHI* could endanger the *individual*. (The statement may be oral or written. *Workforce members* can ask *individual*s if disclosure of *PHI* could put them in danger, or *individual*s can fill out a request form that contains a checkbox question about possible endangerment due to *PHI* disclosure). Organization will not require an *individual* to give details of the perceived endangerment.
6. Organization, *when acting as a provider*, will have the *Privacy Officer* promptly review the completed *Request for Communications* form to determine if the request is reasonable.
    a. **Organization** *will not* require an explanation for the request.
    b. **Organization** will not base its decision on the perceived merits (i.e., whether patient has a "good reason" for making the request) of the request.
    c. **Organization** will accommodate a request that it determines is reasonable (administratively feasible). Examples of reasonable requests include:
        i. The use of a sealed envelope rather than a postcard.
        ii. Receiving mail at a P.O. Box or office rather than a home address.
        iii. That telephone reminders only be communicated to an office or cell number."
7. The *Privacy Officer* will complete the Response section of the Request for Communications form to inform the patient of the **Organization's** decision and may suggest different forms of alternate communications for requests that have been found not to be administratively feasible.
8. If the **Organization** grants an *individual*'s request, the decision must be documented by maintaining a written or electronic record of the action taken.

9. The *Privacy Officer* shall maintain all requests and responses in the appropriate location in the *individual*'s *medical record* and *workforce members* must review the record when communicating with the *individual*.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.502(c) *Uses and Disclosures of PHI Subject to an Agreed Upon Restriction*
45 CFR 164.502(h) *Confidential Communications*
45 CFR 164.522 *Rights to Request Privacy Protection for Protected Health Information*

Privacy Policy 17.0 Individual Right: Request Amendment of Designated record set

FULL POLICY LANGUAGE:

Policy Purpose:
It is the policy of **Organization** to honor an *individual*'s right to request an *amendment* or correction to their protected health information held in their *designated record set*, establish a process to review, deny, allow, and implement *amendment*s and reflect requests for *amendment*s in our records, and to notify others known by the **Organization** to have the information in their records.

Workforce members, *business associates*, and other healthcare *providers* must all comply with this policy.

Policy Description:
The *HIPAA* Privacy Rule grants *individual*s the right to *amend* or supplement their own protected health information, for as long as a *covered entity* (**Organization**) maintains the *PHI* in a *designated record set*. The right to *amend* includes the right to correction of errors, and the right to supplement an existing record with additional *PHI*. A *designated record set* is a group of records maintained by or for **Organization,** which includes billing records, *medical record*s, and other records **Organization** uses to make decisions about *individual*s.

Organization will establish a process to review, allow, deny, and reflect *amendment*s and requests for *amendment*s in the *designated record set* and to notify others known by the **Organization** to have the information in their records.

Procedures:
Requests to be in Writing:
Individual requests for *amendment* of protected health information shall be made in writing to **Organization** and clearly identify the information to be *amend*ed, as well as the reasons for the *amendment* and the content of the *amendment*.

Responding to a Request for *Amendment* or Notification of an *Amendment*:
Timing:
Organization must act on an *individual*'s request for *amendment* no later than 60 days after it receives the request. The deadline may be extended up to 30 days if **Organization** provides the *individual* with a written statement of the reasons for delay and the date by which **Organization** will fulfill his or her request before the expiration of the sixty days. The final response must be provided no later than 90 days from the date of the request.

Organization will promptly act upon a notice of an *amendment* for records in its *designated record set* received from another *covered entity*

Implementation of *Amendment*: Notice from Another *Covered entity*
Upon receipt of notice from another *covered entity* of an *amendment* to records authored by that *covered entity* but also held in **Organization's** records, **Organization will** identify the information in the *designated record set* to be *amend*ed and clearly reflect the *amendment* in the *designated record set* for as long as it is held by the **Organization** and whenever it is shared by the **Organization.** Additionally, **Organization** will inform its *business associates*, that may use or rely on the *individual*'s *designated record set*, of the *amendment*, so that they may make the necessary revisions based on the *amendment*.

Review *Amendment* Request:
Privacy Officer or their designee will be responsible for reviewing all requests for *amendment*s in a timely manner and in accordance with the guidelines below. Reviewer will involve clinical resources as necessary and the author of the record when appropriate.

It may be determined that a further review of the patient's request for *amendment* could be aided by the participation of an uninvolved third party. For purposes of this policy, an uninvolved third party will be defined as an individual who has not been involved in the original review of the request. This individual should be in a leadership position which, for the purposes of this policy, includes (but are not limited to) risk management officers, executive leaders and medical staff leadership.

Allowing Request for *Amendment*:
If **Organization** approves the request for *amendment*, **Organization** must timely inform the *individual* that the request to *amend* has been accepted, and then make the appropriate *amendment*, reflecting it in the *designated record set* as well as timely notifying others known by the **Organization** to have the information in their records.

If **the request is granted,** after review and approval by the individual responsible for the entry to be *amend*ed, **Organization** must:

- Insert the *amendment* or provide a link within the *designated record set* to the *amendment* at the site of the information that is the subject of the request for *amendment*;
- Inform the *individual* that the *amendment* is accepted;
- Obtain the *individual*'s identification of, and agreement to, have the **Organization** notify the relevant persons with whom the *amendment* needs to be shared. These persons include:
    - Persons identified by the *individual* as having received protected health information about the *individual* and needing the *amendment*; and
    - Persons, including *business associates*, that the **Organization** knows have the protected health information that is the subject of the *amendment* and that may have relied, or could foreseeably rely, on such information to the detriment of the *individual*.

Organization must then provide the *amendment* to both entities identified by the *individual*, and other entities known to have received the erroneous information.

Denial of Request for *Amendment*:
Organization may deny an *individual*'s request for *amendment* **only** *when the reviewer* determines that the information or record:

1. Was not created by **Organization**, unless the originator of the protected health information is no longer available to make the *amendment*;
2. Is not part of a *designated record set*;
3. Would not be available for inspection (under the Privacy Rule "right of *access*" standard) See Privacy Policy 15, *Right to Access* for further details;
4. Is accurate and complete.

If **Organization** denies an *individual*'s request, it must give the *individual* a timely, written denial, which includes:

1. The basis for the denial;
2. The *individual*'s right to submit a written statement disagreeing with the denial and how to exercise that right;
3. A statement that the *individual* can request that **Organization** include the *individual*'s request and the denial with any future disclosures of the information (so long as the *individual* does not file a statement of disagreement – see below for process when one is filed); and
4. A description of how the *individual* can file a complaint with **Organization** or the Secretary of the Department of Health and Human Services (*HHS*).

Statements of Disagreement:
If **Organization** denies all or part of a requested *amendment*, **Organization** must permit the *individual* to submit a written statement disagreeing with the denial of all or part of the

requested *amendment*, and the basis of such disagreement. **Organization** may reasonably limit the length of such statement.

Organization may prepare a written rebuttal to the *individual*'s statement of disagreement. Whenever such a rebuttal is prepared, **Organization** must provide a copy to the *individual* who submitted the statement of disagreement.

Recordkeeping for Disputed *Amendment*s:
Organization must, as appropriate, identify the record or protected health information 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*, **Organization's** denial of the request, the *individual*'s statement of disagreement, if any, and **Organization's** entity's rebuttal, if any, to the *designated record set*.

Documentation:
Organization must document the titles for the persons or offices responsible for receiving and processing requests for *amendment*s and retain the documentation as required by the *HIPAA* Privacy Rule for at least six years.

RELEVANT *HIPAA* REGULATIONS:

45 CFR 164.528 *Accounting of Disclosures of Protected Health Information*

Privacy Policy 18.0 Individual Right: Accounting of Disclosures

FULL POLICY LANGUAGE:

Policy Purpose:
The purpose of this policy is to ensure *individual*s can receive an *accounting of disclosures* of their protected health information.

Policy Description:
Organization, upon an *individual*'s request, will provide the *individual* with an accounting of certain disclosures of *PHI*. This policy details the required content of an *accounting of disclosures* that should include at least the following information: all non-excluded disclosures, including those made by a *business associate*, for a period not to exceed six years (can be for a shorter time at the request of the *Individual*). It must also include details like the date, name of entity/person receiving the phi, their address (if known), brief description of the disclosed information, and a copy of the request or a statement of reason for disclosure. For instances of multiple disclosures to same entity, the details may be limited to the first disclosure and a list of frequency or number of disclosures made during the accounting period and the date of the last disclosure. *Research* disclosures should also be included with details of the *research* and disclosures and an offer to help contact the *researche*r if desired. *Privacy Officer* will handle all

requests for *accounting of disclosures* and may delegate the responsibility at his or her discretion.

Disclosures Not to Be Included in an Accounting:

In response to a request for an *accounting of disclosures***, Organization** will exclude the following disclosures:

1. made for *treatment*, *payment*, and healthcare operations
2. to the *individual* themself;
3. made incident to another allowed or required disclosure;
4. made pursuant to a valid authorization;
5. for facility directories, to those involved in the *individual*'s care or those involved in their care and those made for notification purposes, including identifying and locating a family member;
6. for national security or intelligence purposes;
7. made to law enforcement or correctional institutions with lawful custody of an inmate;
8. made as a part of a *limited data set*;
9. to which a valid request for delayed accounting by law enforcement or a health oversight agency is in place and has not expired; and
10. made more than six years prior to the date of the request for an accounting.

Required Disclosures:
In response to a request for an *accounting of disclosures*, **Organization** will include disclosures

1. made as required by law (i.e., reporting of certain wounds)
2. made for public health activities;
3. made for health oversight activities;
4. made to report victims of abuse, neglect, and domestic violence;
5. made for judicial and administrative proceedings;
6. made for *research* conducted under an *Institutional Review Board* (*IRB*) Waiver of Authorization;
7. made to avert a serious threat to the health and safety of the *individual*, or to the public;
8. made for certain specialized government functions (i.e., military and veterans affairs; medical suitability determinations); and
9. made for workers' compensation purposes.

Required Tracking:
Organization will maintain and track the following information for disclosures that could be included in an accounting:

1. The date of disclosure;
2. The name of the *individual* or entity who received the information and their address, if known;

3. A brief description of the protected health information disclosed;
4. A brief statement of the purpose of the disclosure.
5. Multiple disclosures to the same party for a single purpose may have a summary entry. A summary entry includes all information for the first disclosure, the frequency with which disclosures were made, and the date of the last disclosure.
6. **Organization** will maintain summary information for all public health authority reviews of its entire record set, or the portion of the entire record set that was made available for review but need not reflect these reviews in each individual record that may have been accessed. **Organization** will maintain these summaries in a way that makes it easy to reflect them in any *accounting of disclosures* for *individual*s.

Procedures:

Processing the Request:

1. All requests for an *accounting of disclosures* must be submitted, in writing, to the **Organization**.
2. The **Organization** must retain this request, retain a copy of the written account to be provided to the patient, and maintain a record of the name/departments responsible for the completion of the accounting or of the *Privacy Officer* if it was not delegated.
3. *Individual*s may authorize in writing that the *accounting of disclosures* be released to another individual or entity. The request must clearly identify all information required to carry out the request (name, address, phone number, etc.).
4. The **Organization** must retain all requests, maintain a copy of the written account to be provided to the third party, and maintain a record of the name/departments responsible for the completion of the accounting or of the *Privacy Officer* if it was not delegated.

Gathering the Necessary Information:

Upon receipt of a completed request for *accounting of disclosures* form, the **Organization** will gather the requested information by:

1. Querying all systems and searching any records not in electronic form that contain disclosures that are not excluded from *accounting of disclosures*;
2. Obtaining a Disclosure Report from all departments that maintain such reports;
3. Contacting *business associates*, as necessary, to request any pertinent disclosures made by or through them to include in the accounting.

Preparing the *Accounting of disclosures*:

Accountings of disclosures shall be prepared by **Organization** following the protocol listed for each type of disclosure:

1. For each individual item on the *accounting of disclosures* **Organization** will include:
    a. The date the disclosure was made;

b. The name of the entity or person receiving the *PHI*, and, if known, the address of such entity or person (to the extent revealing this information does not violate the *HIPAA* regulations);
c. A brief description of the *PHI* that was disclosed; and
d. A brief description of the purpose of the disclosure; OR
e. For multiple disclosures to the same person or entity for the same purpose during the accounting period, A summary entry includes all information for the first disclosure, the frequency with which disclosures were made, and the date of the last disclosure.

2. Organization need not note in each individual record when it discloses all its records or a portion of its records that included the *individual* for public authority oversight activities, but these disclosures must be included in the *accounting of disclosures* with a summary of the dates the records were made available, the entity and/or person who may have reviewed the record and a brief description of the purpose of the disclosure; and

3. Each disclosure made to an external *researche*r for a particular *research* purpose involving 50 or more *individual*s under an *Institutional Review Board* waiver of authorization will include:
    a. The name of the protocol or other *research* activity;
    b. A brief 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;
    c. A brief description of the types of *PHI* that were disclosed;
    d. The date or period of time during which disclosures occurred;
    e. The name, address, and telephone number of the entity that sponsored the *research* and of the *researche*r to whom the information was disclosed; and
    f. A statement that the *PHI* of the patient may or may not have been disclosed for a particular protocol or *research* activity;
    g. An offer to help the *individual* at their request to contact the *researche*r and the entity that sponsored the *research*.

Sending the Accounting and Timing:

1. In accordance with the *HIPAA* regulations, **Organization** will provide the *individual* with an accounting within 60 days after receipt of the request.
2. If the accounting cannot be completed within 60 days after receipt of the request, prior to the expiration of the 60 days, **Organization** will provide the *individual* with a written statement of the reason for the delay and the expected completion date. Only one extension of time, 30 days maximum, per request is permitted.
3. In no event will **Organization** provide the *individual* with the accounting later than 90 days from the date of the request.
4. The **Organization** will provide an accounting for a period of time of up to six years prior to the date of the request, unless the *individual* specifies a shorter time frame.

5. **Organization** must provide an accounting to the *individual* at no charge for the first request made during any twelve-month period.
6. A reasonable fee can be charged for any additional requests made during a twelve-month period, *provided* that the *individual* is informed of the fee in advance and given an opportunity to withdraw or modify the request.

Maintaining Records of Accountings Provided:
Organization must maintain all information subject to an accounting for at least six years, or longer (if required by **Organization's** state).
Organization must maintain written requests for an accounting provided to an *individual* for at least six years from the date it was created, or longer (if required by **Organization's** state).
Organization must maintain the titles and names of the people responsible for receiving and processing accounting requests for a period of at least six years, or longer (if required by **Organization's** state).

RELEVANT *HIPAA* REGULATIONS:

45 CFR 164.528 *Accounting of Disclosures of Protected Health Information*

Privacy Policy 19.0 Uses and Disclosures: Psychotherapy *notes*

FULL POLICY LANGUAGE:

Policy Purpose:
To ensure *workforce members* understand the distinction between *psychotherapy notes* and other mental health records, the mental health practitioner/patient privilege that applies to *psychotherapy notes* in most states, and the requirement that these notes be separated from the *designated record set* to receive heightened protections. To assure that Organization follows all requirements for use and disclosure of *psychotherapy notes* in the limited circumstances where it is allowed.

Policy Description:
This policy describes how **Organization** is to respond to requests for *psychotherapy notes*; the distinction between *psychotherapy notes* and other mental health records; the mental health practitioner/patient privilege that applies to *psychotherapy notes*; and the requirement that these notes be separated from the *designated record set* to receive heightened protections. The Policy also describes the processes Organization will follow to assure that it meets all requirements for use and disclosure of *psychotherapy notes* in the limited circumstances where it is allowed.

Procedures:

What are *Psychotherapy notes*?

Organization will treat notes recorded in any medium by a health care *provider* who is a mental health practitioner documenting or analyzing the contents of a conversation during a during a private counseling session or a group, joint, or family counseling session that are separated from the rest of the *medical record* as *psychotherapy notes*.

Separation from *Designated record set*
Organization will provide a means for recording any *Psychotherapy notes* in its possession separately from the *designated record set* in order to preserve the heightened privacy afforded these records. This separation may be electronic or physical.

What is not included in *Psychotherapy notes* even though it is related to psychotherapy?
Organization will not consider the following as *psychotherapy notes*: medication prescription and monitoring, session start and stop times, modalities and frequency of *treatment*, clinical test results, or summary information on diagnosis, functional status, *treatment* plan, symptoms, prognosis and progress to date. Organization will consider this content part of the mental health record and recognizes that heightened privacy requirements may apply because it is sensitive *PHI* under most state laws.

***Psychotherapy notes* and the Mental Health Practitioner/Patient Privilege**
If there is a practitioner/patient privilege that attaches to *psychotherapy notes* under applicable state law, **Organization** will honor that privilege and require that the privilege be validly waived in any situation in which another law does not take priority over this privilege.

Use of Legal Counsel
Organization will seek legal counsel when it is unsure of how to proceed prior to releasing *psychotherapy notes*.

Limitations on Use and Disclosure of *Psychotherapy notes* for *Treatment*
Psychotherapy notes are treated differently from other mental health information both because they contain particularly sensitive information and because they are the personal notes of the therapist that typically are not required or useful for *treatment*, *payment*, or *health care operations* purposes, other than by the mental health professional who created the notes. Accordingly, **Organization** will follow the rule that only the originator of the *psychotherapy notes* may *access* those notes for the *treatment* of the *individual* to which they apply unless the privilege has been waived and a valid authorization has been signed by the *individual*.

Patient *Access* to *Psychotherapy notes*:
Even though the patient has a right to *access* most health information, the patient does not have a right to *access psychotherapy notes*. Therefore, the **Organization** is not required to fulfill a patient's request for *access* to *psychotherapy notes*. However, the **Organization** will inform the patient of this limitation in response to a request for *access*.

Patient Authorization Required:

In most circumstances, the **Organization's *Workforce members*** must obtain a patient's written authorization for any use or disclosure of *psychotherapy notes*. If there is a concern that a request for disclosure is unnecessary or excessive, the **Organization** may ask the patient if the authorization for disclosure is consistent with his or her wishes.

Organization will utilize an Authorization for the use or disclosure of *psychotherapy notes* specific to the *psychotherapy notes* and may not combine the authorization with any other consent or authorization with the exception of another authorization for the use or disclosure of *psychotherapy notes*.

Patient Authorization *Not* Required: The **Organization** is not required to obtain an authorization for the following uses or disclosures of *psychotherapy notes*, when use or disclosure is necessary to:

1. To carry out the following *treatment*, *payment*, or *health care operations*:
    a. Use by the originator of the *psychotherapy notes* for *treatment*;
    b. Use by the **Organization** for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or *individual* counseling; or
    c. Use by the author of the notes or the **Organization** to defend the author, the Organization or another *member* of Organization's *workforce* in a legal action or other proceeding brought by the *individual* who is the subject of the notes. Such use is not allowed in response to a legal action brought by anyone other than the *individual* who is the subject of the notes.
2. To respond to the federal Department of Health and Human Services (*HHS*) to determine the **Organization's** compliance with *HIPAA* privacy rules;
3. To comply with the law;
4. To assist in health oversight activities regarding the originator of the *psychotherapy notes*;
5. To help coroners/medical examiners in the examination of deceased persons; and
6. To prevent or lessen a serious and imminent threat to the health or safety of a person or the public. Organization will only make such disclosures when necessary in the professional judgement of the author of the notes and when made to a person reasonably able to prevent or lessen the threat. **Organization** will follow state law in determining whether such disclosures are mandatory or permissive.

RELEVANT *HIPAA* REGULATIONS:

45 CFR 164.508(a)(2) *Uses and Disclosures for Which an Authorization is Required: Psychotherapy notes*

Privacy Policy 20.0 Minors' Rights

FULL POLICY LANGUAGE:

Policy Purpose:

To set forth **Organization's** requirements surrounding *access* to an unemancipated minor's records and *PHI*.

Policy Description:

This policy describes circumstances in which Organization will require minors to *access* their *PHI* through a *personal representative*, and when minors may *access* their *PHI* directly with or without the approval or knowledge of parents, guardians or *personal representative*s. It also describes the circumstances in which Organization will require a minor's approval for parents, guardians and *personal representative*s to *access* a minor's record.

This policy further describes the circumstances under which **Organization** *must* provide minors with *access* to their *PHI*; when **Organization** *may* do so; and when **Organization** *may not* do so.

Procedures:

Exercising *HIPAA* rights and *Access* to Minor's *PHI*

When Parents guardians or other person acting in loco parentis are *Personal representative*

Although generally, Organization may regard a parent, guardian or other person acting in loco parentis of a minor child as what the *HIPAA* Privacy Rule *personal representative*, there are also number of situations where that the **Organization** may not do so.

Because parents, guardians and those acting in loco parentis do not have unfettered rights to act as *personal representative*s, Organization will determine their rights on a case-by-case basis. Organization will honor a parent who is a *personal representative* exercise of a minor's *HIPAA* Privacy Rule rights with respect to protected health information (*PHI*) and other *HIPAA* rights like the signing of authorizations, consistently with state and other laws in the following circumstances:

1. a *personal representative* has the authority to act on behalf an emancipated minor in making decisions related to healthcare, **Organization** must treat that person as a *personal representative*, with respect to *PHI* unless otherwise prohibited (see discussion below regarding abuse, neglect and endangerment);
2. If, under applicable law, a parent, guardian, or other person acting *in loco parentis* has the authority to act on behalf of an unemancipated minor in making decisions related to healthcare, **Organization** must treat that person as a *personal representative* with respect to *PHI* relevant to such personal representation unless otherwise prohibited (see discussion below regarding abuse, neglect and endangerment).

Honoring the Minor's authority to Act

The Organization may not treat another person as a representative of the unemancipated minor, and must honor the minor's authority to act as an *individual* with respect to *PHI* pertaining to health care services, if under federal, state or other applicable law, including case law:

1. The minor consents to such healthcare services; *no other consent is required by law*, regardless of whether the consent of another person has been obtained; and the minor has not requested that person be treated as the *personal representative*;
   Example: A state law provides an adolescent the right to obtain mental health *treatment* without the consent of his or her parent, and the adolescent consents to such *treatment* without the parent's consent.
2. The minor may lawfully obtain such health care services without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service;
   Example: A court may grant authority to make health care decisions for the minor to an adult other than the parent, to the minor, or the court may make the decision(s) itself.

   or when

3. A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between **Organization** and the minor with respect to such healthcare service.
   Example: A physician asks the parent of a 16-year-old if the physician can talk with the child confidentially about a medical condition and the parent agrees.

What Role Does State and other Federal Law Play?
The *HIPAA* Privacy Rule does not contravene state or other federal laws that expressly address the ability of parents to obtain health information about minors.

For example, regardless of whether a parent is the *personal representative* of a minor child, the *HIPAA* Privacy Rule permits a *covered entity* to disclose to a parent, or provide the parent with *access* to, a minor child's protected health information, *when and to the extent* it is permitted or required by state law.

Likewise, the *HIPAA* Privacy Rule prohibits **Organization** from disclosing a minor child's protected health information to a parent, or providing a parent with *access* to such information, when and to the extent it is prohibited under state or federal law.

Situations involving Endangerment Domestic Violence, abuse or Neglect

When **Organization** reasonably believes that an *individual*, including an unemancipated minor, has been or may be subjected to domestic violence, abuse, or neglect by the *personal representative*, or that treating a person as an *individual*'s *personal representative* could endanger the *individual*, **Organization** may choose not to treat that person as the *individual's*

personal representative, if in the exercise of professional judgment, doing so would not be in the best interests of the *individual*. See the paragraph discussing *personal representative*s in Privacy Policy 17.0: *Uses and Disclosures: General Rules* for more detail.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.502(g) *Personal Representatives, Adults and Emancipated Minors*

Privacy Policy 21.0 Use of Social Media

FULL POLICY LANGUAGE:

Policy Purpose:

To provide rules for acceptable social media use.

Policy Description:

This policy outlines the safeguards *Workforce members* must follow to ensure that their use of social media does not result in unauthorized disclosure of *PHI*.

Procedures:

The following principles apply to professional use of social media on behalf of **Organization**, as well as personal use of social media when referencing the **Organization** or anyone served by them.

***Individual* Privacy** (*individual*s include patients, persons served, beneficiaries and insureds and the term is further defined in the Glossary)**:**

1. Posting an *individual*'s information, commentary, or photographs on professional or personal social media sites requires written authorization from the *individual*.
2. *Workforce members* should contact their supervisors, or the *Privacy Officer*, to obtain a copy of the form.
3. Once the form is obtained, a copy of the form is provided to the *individual* and the original authorization is placed in the *individual*'s *medical record*.
4. Members of the *workforce* may not live stream, audio record or video -record in *treatment* areas, unless written permission is given by the *Privacy Officer*, the *provider*(s) and the *individual*s involved.
5. If any photos, audio recordings, or video-recordings, contain images or recordings of more than one *individual*, written authorization from all *individual*s those patients must also be obtained.
6. **Organization** staff and *providers* may not live stream or take personal photos, video or audio recordings in health care areas, so as to avoid inadvertently capturing *individual*s or their information.
7. Photos, images or a narrative a *workforce member* believes to be de-identified may in fact be recognizable by an *individual* or someone who knows of them. Therefore, permission should be obtained from the *Privacy Officer* prior to posting any photos,

images or narratives involving *individual*s or their information even if they are thought to be de-identified.

8. *Providers* may video or audio record *individual*s for *treatment* purposes, after receiving their written authorization. Such recording may only be made using electronic devices that have been approved for such purpose by the Security Officer.
9. *Workforce members* who suspect unauthorized disclosure of an *individual*'s information via social media, or any suspected unauthorized live streaming, photographing, filming, or recording, shall promptly report such suspicions to the *Privacy Officer*.

Interacting with *Individual*s on Social Media

1. *Workforce members* may not connect with *individual*s or their family *members* using social media.
2. *Workforce members* should not accept "Friend" requests from *individual*s on social media sites such as Facebook, nor should *workforce members* send such requests.
3. For situations in which an *individual* is a relative, household *member* or other acquaintance of the *workforce member* and the *individual* and the *workforce member* had an established relationship prior to interacting at the **Organization**, the *Privacy Officer* or their designee will review such situations on a case-by-case basis to determine whether or not to exempt certain social media activity between them from this policy. Such exemption will not include the posting of any *PHI* without the *individual*'s express written authorization regardless of the relationship between the parties.

RELEVANT HIPAA REGULATION:

45 CFR 164.530(c) *Privacy Safeguards*

Privacy Policy 22.0 Uses and Disclosures: Response to Judicial and Administrative Proceedings

FULL POLICY LANGUAGE:

Policy Purpose:

To establish rules for how **Organization** will respond to requests for disclosure of *PHI* in the course of judicial or administrative proceedings through judicial or administrative orders, subpoenas, discovery requests, or other lawful process, that is not accompanied by an order of a court or *administrative tribunal*. **Organization** will cooperate with courts and with counsel to provide lawfully sought *PHI*, while simultaneously ensuring protection of *individual* privacy.

Policy Description:

Organization may receive requests to disclose *PHI* in the course of judicial or administrative proceedings. Requests can be in the form of a subpoena, court order, request for discovery, or other lawful process not accompanied by an order of a court or an *administrative tribunal*. This policy outlines how to handle disclosures of *medical record*s and other health information for purposes of judicial and administrative hearings. In the absence of an actual order but with

lawful process (for example a subpoena or discovery request), **Organization** will determine if there is satisfactory assurance that the *individual* received appropriate notice and a chance to respond or to provide notice prior to releasing protected health information. **Organization** may determine if there are grounds for objection to a judicial or administrative order prior to responding, especially where the request seems overly broad or irrelevant.

Procedures:

Disclosing *PHI* in Response to a Court or Administrative Order:

If the **Organization** receives an order from a court or administrative judge requiring **Organization** to disclose protected health information, **Organization** may only release that *PHI* which the order expressly authorizes disclosure.

If the Organization feels the order may be overbroad, irrelevant or objectionable on other legal grounds, the *Privacy Officer*, working with legal counsel, may review any such order to determine whether **Organization** will object to the order on any lawful basis. If the Organization concludes that an objection to the order is required, such objection shall be filed in accordance with applicable state or federal law and filing deadlines. The objection shall be documented.

Disclosing *PHI* in Response to a Subpoena, Discovery Request, or Other Lawful Process Other Than a Court Order:

1. The **Organization** may release *PHI* in response to a subpoena, discovery request, or other lawful process, that is not accompanied by a court order, as follows:
    a. The **Organization** may release *PHI* if it receives ***written*** "satisfactory assurance" from the party requesting the information that reasonable efforts have been made by the requesting party to ensure that the patient who is the subject of the *PHI* has been given notice of the request. Receipt of "Satisfactory assurance" that the requesting party has made a good faith effort to notify the *individual* of the request for is met where the requesting party provides the **Organization** a *written statement and supporting documentation* demonstrating that:
    b. The requesting party has made a good faith attempt to provide written notice to the *individual* (if the *individual*'s location is unknown, documentation showing that a notice was mailed to their last known address shall be provided by the requesting party);
    c. The requesting party provided notice to the *individual* containing enough information to allow the *individual* to make an informed objection to the court or *administrative tribunal* regarding the release of their *PHI*; and
    d. The time for the *individual* to raise objections to the court or *administrative tribunal* has passed, and, either no objections were filed, **or** all objections filed by the *individual* have been resolved and the disclosures being sought are consistent with the court's resolution.
2. The **Organization** may release *PHI* to a requesting party if it receives ***written*** satisfactory assurance from the requesting party that reasonable efforts have been made by such party to secure a *qualified protective order*. A *qualified protective order* is an order of a court or *administrative tribunal* or a stipulation by the parties to the proceeding, that

prohibits the parties from using or disclosing *PHI* for any purpose other than the proceeding for which the information was requested. A qualified protective order requires the parties to return the *PHI* (including all copies made) to **Organization** at the end of the proceeding.

   a. "Satisfactory assurance" in this instance means that the **Organization** has received from the requesting party a written statement, along with supporting documentation, demonstrating that:

3. The parties to the dispute giving rise to the request for *PHI* have *agreed* to a qualified protective order and have presented it to a court or *administrative tribunal* with jurisdiction over the dispute; or
4. The requesting party has asked for a qualified protective order from such court or *administrative tribunal*.
5. The **Organization** may release *PHI* to a requesting party even without satisfactory assurance from that party if the **Organization** either:
   a. Makes reasonable efforts to provide notice to the *individual* about releasing their *PHI*, so long as the notice meets all of the following requirements:
      i. The notice is written and given to the *individual* (if the *individual*'s location is unknown, **Organization** should establish documentation showing that a notice was mailed to their last known address);
      ii. The notice contained enough information to allow the *individual* to make an informed objection to the court or *administrative tribunal* regarding the release of their *PHI*; and
      iii. The time for the *individual* to raise objections to the court or *administrative tribunal* has lapsed and either no objections were filed, or all objections filed by the *individual* have been resolved and the disclosures being sought are consistent with the court's resolution.
   b. Seeks a qualified protective order from the court or *administrative tribunal* or convinces the parties to stipulate to such order.

RELEVANT *HIPAA* REGULATIONS:

45 CFR164.512(e) *Use and Disclosure of Protected Health Information for Judicial and Administrative Proceedings*

Privacy Policy 23.0 Uses and Disclosures: Fundraising

FULL POLICY LANGUAGE:

Policy Purpose:

To ensure **Organization conducts any** *fundraising* activities consistent with the Privacy Rule.

Policy Description:

If **Organization** notifies *individual*s in its Notice of Privacy Practices that it may conduct *fundraising* activities, **Organization** may conduct *fundraising* activities for its own benefit that

disclose information listed below, without written *individual* authorization. *Fundraising* activities that disclose more than the information listed below require written *individual* authorization. All *fundraising* materials must describe how an *individual* can opt out of receiving future *fundraising* communications. **Organization** will make reasonable efforts to comply with *opt-out* requests.

Procedures:

1. **Organization**, when *fundraising* for its own benefit, may use or disclose, without written *individual* authorization, the following *PHI* to a *business associate* or to an institutionally related foundation (such as a nonprofit charitable foundation):
    a. Demographic information related to an *individual* including name, contact information, gender, date of birth and age;
    b. Dates of health care provided to an *individual*;
    c. The department (if any) where services were received;
    d. Treating physician;
    e. Outcome information; and
    f. Health insurance status.
2. **Organization's** Notice of Privacy Practices must include the following information:
    a. **Organization** or its *agent* may contact a patient to raise funds for **Organization**; and
    b. The patient may opt out of receiving any *fundraising* communications.
3. Any *fundraising* that **Organization** sends to an *individual* must describe how the *individual* may opt out of receiving any further *fundraising* communications, providing the *individual* with a clear and conspicuous opportunity to elect not to receive any further *fundraising* communications. The method for opting-out may not cause the *individual* to incur an undue burden or more than a nominal cost.
4. If an *individual* elects to opt out, the **Organization** may not make additional *fundraising* communications to the *individual*.
5. **Organization** may provide an *individual* with a means to opt back in to *fundraising* communications at the *individual*'s request.
6. If the *fundraising* is not for the **Organization's** benefit, or includes more than the information listed above, a written authorization from the *individual* is required.

Opting-Out Procedures:

1. **Organization** must make reasonable efforts to ensure that *individual*s who decide to opt out of receiving future *fundraising* communications are not sent such communications.
2. **Organization** may not condition *treatment* or *payment* on the *individual*'s choice with respect to receipt of *fundraising* communications.
3. **Organization** may provide an *individual* who has elected not to receive further *fundraising* communications with a method to opt back in to receive such communications.
4. If an *individual* has given written authorization for *fundraising*, that *individual* has the right to revoke the authorization, and may do so in writing.

5. The **Organization's** *fundraising* department, institutionally related foundation, or *business associate* will maintain a log of all *individual*s and others who have either revoked a *fundraising* authorization or opted-out of receiving future *fundraising* communications.
6. Upon receipt in writing or other written notification that the *individual*'s *fundraising* authorization has been revoked, the **Organization** may not send additional *fundraising* communications to them.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.514(f)(2) *Uses and Disclosures for Fundraising & Implementation Specifications: Fundraising Requirements*
45 CFR 164.501 *Definitions*

Privacy Policy 24.0 Uses and Disclosures: Workers Compensation

FULL POLICY LANGUAGE:

Policy Purpose:

To provide rules for use or disclosure of *PHI* for workers compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

Policy Description:

HHS guidance makes clear that the Privacy Rule recognizes legitimate needs for insurers and other entities involved in the worker's compensation system to be allowed *access* to an *individual*'s *PHI* when authorized by state or other law. These laws may vary significantly so the Privacy Rule permits disclosure of *PHI* for worker's compensation purposes in a number of ways including allowing disclosures without an *individual*'s authorization, allowing disclosures with an *individual*'s authorization, and requiring the application of the *minimum necessary standard* for worker's compensation disclosures.

Disclosures made for Worker's Compensation related *medical record*s without an *individual*'s authorization.

The Privacy Rule permits **Organization** to, and the **Organization** will disclose protected health information to workers' compensation insurers, State administrators, employers, and other persons or entities involved in workers' compensation systems, without the *individual*'s authorization:

1. When such release is authorized by and to the extent necessary to comply with laws relating to workers' compensation or similar programs established by law that provide benefits for work-related injuries or illness without regard to fault. This includes programs established by the Black Lung Benefits Act, the Federal Employees' Compensation Act, the Longshore and Harbor Workers' Compensation Act, and the Energy Employees' Occupational Illness Compensation Program Act. See 45 CFR 164.512(l).

2. To the extent the disclosure is required by State or other law. The disclosure must comply with and be limited to what the law requires. See 45 CFR 164.512(a) for specific limitations.
3. For purposes of obtaining *payment* for any health care provided to the injured or ill worker. Organizations Use and Disclosure requirements for *payment* must be followed.

Disclosures made to Entities and People involved in addressing Worker's Compensation related claims and conditions with an *Individual*'s Authorization

An *individual* may also authorize the Organization to release their *PHI* to worker's compensation insurers and others involved in worker's compensation systems. For release under such an authorization, the authorization must be valid and meet the requirements set forth in Privacy Policy 13: *Uses and Disclosures for which an Authorization is Required*. concerning the validity of an authorization. Organization will not release information beyond the authorization except as otherwise required and to the extent necessary to comply with laws related to worker's compensation and similar programs.

Examples of when an *individual*'s authorization may be required are releases of *PHI* that are not reasonably related to the condition for which they are claiming worker's compensation and are beyond the requirements of the laws applying to record release for worker's compensation purposes.

Application of the *Minimum Necessary Standard* to Disclosures for Worker's Compensation Purposes

Organization may share information for worker's compensation purposes to the full extent authorized by the state or other law and will limit the information to the minimum necessary to meet the legal requirements. Organization will reasonably rely on a state worker's compensation official or other public official's representations that the information requested is the minimum necessary for the intended purpose.
Organization will also limit the information shared for receiving *payment* for services performed related to a worker's compensation claim to the minimum necessary for that purpose.

Procedures:

1. After receipt of written request from an *individual*, employer, state board of workers compensation, or workers compensation insurance carrier for the employer, **Organization** shall release, within a reasonable amount of time and no later than required by the applicable legal requirements, copies of *medical record*s or verbal communications, that reasonably relate to the work injury in compliance with the *minimum necessary standard* and with the law requiring the disclosure. If Organization finds that is routinely making such disclosures, it may develop a standard protocol to be used for meeting the Minimum Necessary standard for worker's compensation *payment* disclosures.

2. Requests for copies of *medical record*s, which extend beyond the scope of the work-related injury and the reach of the applicable law, need to be accompanied by a valid written authorization from the *individual*.
3. **Organization** shall furnish legible duplicates of written material requested by *individual*s, employers, insurance carriers, and state boards of workers compensation. Certified copies shall be furnished upon request.
4. **Organization** will follow this same process for the release of *PHI* for *workforce members* who have filed a claim under worker's compensation or related laws for on the job related injury or conditions**.**

RELEVANT *HIPAA* REGULATIONS:

45 CFR 164.512(l) *Uses and Disclosures for which an Authorization or Opportunity to Agree or Object is Not Required: Worker's Compensation*

Privacy Policy 25.0 Uses and Disclosures: Limited Data Set and Data Use Agreements

FULL POLICY LANGUAGE:

Policy Purpose:

To establish the process for creating a Limited Data Set, as well as the purposes for and circumstances under which a Limited Data Set may be disclosed. To describe the process for creating the Data Use Agreement that must be signed before sharing a Limited Data Set.

Policy Description:

This policy defines a *limited data set*; sets forth appropriate uses for *limited data set*s; requires that a data use agreement meeting the defined criteria be in place between the parties; requires that the **Organization** adhere to applicable data use agreements and monitor the recipient's use of the data set for patterns of activity or practices in violation of the data use agreement, and requires **Organization** to end sharing of the data set and report to *HHS* if any violations are not reasonably cured.

Under *HIPAA*, a *limited data set* is a set of identifiable healthcare information. The *HIPAA* Privacy Rule permits **Organization** to share a *limited data set* with certain entities for *research* purposes, public health activities, and healthcare operations, without having to obtain prior written patient authorization, *if* certain conditions are satisfied.

Since a *limited data set* is still identifiable protected health information, a *limited data set* may only by shared by **Organization** with entities that have signed a data use agreement with **Organization**. A data use agreement allows **Organization** to obtain satisfactory assurances that the *PHI* will only be used for specific purposes; that the *PHI* will not be disclosed by the entity with which it is shared; and that the *HIPAA* Privacy Rule requirements will be observed.

Procedures:

Limited Data Set:

1. **Organization** may disclose a Limited Data Set (*PHI* with certain identifiers removed) to a requesting party only if the disclosure is for purposes of *research*, public health, or *health care operations*.
2. To create a Limited Data Set, the **Organization** (or its *Business associate*) shall remove the following identifiers from existing *PHI* of the *individual*, and of relatives, employers, or household members of the *individual*:
    a. Names;
    b. Street addresses (other than town, city, state and zip code);
    c. Telephone numbers;
    d. Fax numbers;
    e. Email addresses;
    f. Social Security numbers;
    g. Medical records numbers;
    h. Health plan beneficiary numbers;
    i. Account numbers;
    j. Certificate/ license numbers;
    k. Vehicle identifiers and serial numbers, including license plates;
    l. Device identifiers and serial numbers;
    m. URLs;
    n. IP address numbers;
    o. Biometric identifiers (including finger and voice prints); and
    p. Full face photos (or comparable images).
3. The health information that may remain in the Limited Data Set – in the information disclosed – includes:
    a. Dates, including admission dates, discharge dates, service dates, date of birth, and date of death
    b. City, state, and five digit or more zip code
    c. Age (in years, months, days, or hours)
4. Only authorized **Organization** *workforce members*, or authorized *business associates*, may create a Limited Data Set.
5. If a *business associate* creates the Limited Data Set, **Organization** must enter into a *business associate agreement* before the *business associate* can have *access* to the *PHI* or create the L limited Data Set.

Data Use Agreement:

1. **Organization** may use or disclose a Limited Data Set, only if **Organization** first obtains a signed, written Data Use Agreement (DUA) from the person/entity to whom the Limited Data Set is to be disclosed.
2. **Organization** will enter into a DUA must be entered into before there is any use or disclosure of a Limited Data Set to an outside party. **Organization** will abide by the terms of the DUAs and assure that all of its DUAs must:

a. Establish the permitted uses and disclosures of such information by the Limited Data Set recipient. The DUA may not authorize the Limited Data Set recipient to use or further disclose the information in a manner that would violate *HIPAA* privacy requirements, if done by the **Organization**;
b. Establish who is permitted to use or receive the Limited Data Set; and
c. Provide that the Limited Data Set recipient will:
    i. Not use or further disclose the information other than as permitted by the data use agreement DUA or as otherwise required by law;
    ii. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the DUA;
    iii. Report to the **Organization** any use or disclosure of the information not provided for by its data use DUA of which it becomes aware;
    iv. Ensure that any *agent*s 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
    v. Not identify the information or contact the *individual*s.

3. Noncompliance by Limited Data Set Recipient: If at any time **Organization** becomes aware that a recipient of a Limited Data Set has undertaken a pattern of activity or practice that constitutes a material *breach* or violation of the Data Use Agreement, then **Organization** shall take reasonable steps to cure the *breach* or end the violation. If the *breach* cannot be cured or the violation ended, then **Organization** must cease all disclosures of the Limited Data Set to the recipient and report the problem to the Secretary of the Department of Health and Human Services.
4. Minimum Necessary and Accounting for Disclosures: The minimum necessary and accounting for disclosures rules do not apply to *PHI* disclosed as part of a Limited Data Set.

RELEVANT *HIPAA* REGULATION:
45 CFR 164.514(e) *Limited Data Set and Data Use Agreement*

Glossary

Access: Means the ability or the means necessary to retrieve, view, hear, read, write, modify, or communicate records, data or information or otherwise use any system resource.

Accounting of disclosures of PHI: A report that describes a *covered entity*'s disclosures (including those by its *business associates*) of *PHI* other than those disclosures that are excluded from the requirement like those for *treatment*, *payment*, and *health care operations*; those made with written patient authorization; and certain other disclosures.

Administrative tribunal: An officially appointed or elected individual or judge or group of those individuals or judges, including those appointed by administrative agencies who conduct hearings and exercise judgment over specific issues.

Agent: An *agent* of the **Organization** is determined in accordance with federal common law of agency. The **Organization** is liable for the acts of its *agent*s. An agency relationship exists if the **Organization** has the right or authority to control the *agent*'s conduct in the course of performing a service on behalf of the **Organization** (i.e., give interim instructions, direct the performance of the service).

Alternative communications: Information or communications delivered to patients in a manner different than the **Organization's** normal practice. For example, patients may ask for delivery at an alternative address, phone number, or post office box.

Amend/Amendment: The correction of *PHI* or the addition of *PHI* to existing *PHI* contained in a *designated record set*.

Authorization: An *individual*'s written statement of agreement to the use or disclosure of protected health information when that statement includes all required elements.

Breach: The acquisition, *access*, use, or disclosure of protected health information in a manner not permitted which compromises the security or privacy of the protected health information.

Business associate: A person or entity who, 1) is not a *member* of the **Organization's** *workforce* and, 2) provides a service, performs a function, or performs an activity on behalf of a *covered entity* that involves the creation, receipt, maintenance or transmission of protected health information, including but not limited to claims processing or administration, clinical staffing, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, repricing, legal representation and accounting.

Business associate agreement: Under the *HIPAA* Privacy and Security Rules, a *business associate agreement* ("BAA") is a legally binding contract entered into by and between a *covered entity*

and a *business associate*. Among other things, the agreement must contain satisfactory assurances by the *business associate* that the *business associate* will appropriately safeguard protected health information.

Covered entity: A health plan; a health care clearinghouse; or a health care *provider* who stores or transmits any health information in electronic form in connection with a *HIPAA* transaction.

Data aggregation: The act of a *business associate* combining protected health information from multiple *covered entities* in order "to permit data analyses that relate to the *health care operations* of the respective *covered entities*."

De-Identified health information: Health information that does not identify an *individual*, and that does not contain information that can identify or link the information to the *individual* to whom the information belongs.

Designated record set: A group of records maintained by or for a *Covered entity* that is: a) medical and billing records maintained by or for a covered health care *provider* entity; b) enrollment, *payment*, claims, adjudication, and case or medical management record systems maintained by or for a health plan; or c) records used in whole or in part to make care-related decisions.

Disclosure: The release, transfer, provision of *access* to, or divulging in any manner *PHI* to outside the entity holding the information.

Electronic Protected Health Information (*ePHI*): Any *individually identifiable health information* protected by *HIPAA* that is transmitted by or stored in electronic media.

ePHI: any protected health information (PHI) that is created, stored, transmitted, or received in any electronic format or media.

Facility directory: A directory of **Organization's** staff. Patient information may be included in this directory. This information may include patient name, location (room/bed number), condition described in general terms (i.e., "Not feeling well," "Having a good day"), and religious affiliation. Religious affiliation is available to clergy *members* only.

Fundraising: An organized campaign designed to reach out to certain segments of the population to raise monies.

Health care operations. Any of the following activities of a *covered entity* to the extent that the activities are related to a covered function:

7. Quality assessment and improvement activities (including outcome evaluation and clinical guideline development); patient safety; population-based activities related to improving health or reducing health care costs, protocol development, case management and care coordination, contacting health care *providers* and recipients

with information about *treatment* alternatives, related activities that do not include *treatment*;

8. Reviewing the competence, qualifications, performance of health care professionals, health plan performance, conducting health care training programs for students, trainees or practitioners under supervision for practice and improvement of skills; training of non-health care professionals, accreditation, certification, licensing, or credentialing;
9. Underwriting (excluding any use of genetic information), enrollment, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, ceding, securing or placing a contract for reinsurance of healthcare claim risks;
10. conducting or arranging for medical review, legal services, and auditing functions including fraud and abuse detection and compliance programs;
11. business planning and development including formulary development and administration, development or improvement of *payment* or coverage policies;
12. business management and general administrative activities of the entity which include but are not limited to:
    a. Management activities relating to implementation of and compliance with the Privacy Rule;
    b. Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
    c. Resolution of internal grievances;
    d. The sale, transfer, merger, or consolidation of all or part of the *covered entity* with another *covered entity*, or an entity that following such activity will become a *covered entity* and due diligence related to such activity; and
    e. Consistent with the applicable requirements of creating de-identified health information or a *limited data set* and *fundraising* for the benefit of the *covered entity*.

HHS: Stands for the Department of Health and Human Services. This agency is charged with the development, statement, and implementation of the *HIPAA* Privacy Rule.

Health Insurance Portability and Accountability Act (*HIPAA*): Federal legislation passed in 1996, as *amend*ed and updated from time to time, that regulates privacy and security of *individually identifiable health information*.

HIPAA Privacy Rule: The *HIPAA* Privacy Rule regulates the use and disclosure of protected health information. The *HIPAA* Privacy Rule gives *individual*s the right to *access* their protected information; the right to request that this information be *amend*ed; and the right to an accounting of how their *PHI* has been disclosed. The Privacy Rule prescribes measures that must be taken to ensure *PHI* is protected from unauthorized *access*. The Privacy Rule also requires *covered entities* to develop and use Notices of Privacy Practices, which outline how *covered entities* will use or disclose the *PHI* of *individual*s. The Privacy Rule also outlines when

patient written authorization to use or disclose *PHI* is required, and when it is not required. In addition, the Privacy Rule outlines those circumstances under which *PHI* must be disclosed, and those circumstances under which it may not be disclosed.

Individual: The person who is the subject of *PHI*.

Individually identifiable health information: A subset of health information, including demographic information that:

1. Is created or received by a healthcare *provider*, health plan, employer or healthcare clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an *individual*; the provision of healthcare to the *individual*; or the *payment* for the provision of health care for the *individual*; and
3. That identifies the *individual* or might reasonably be used to identify the *individual*.

Institutional Review Board (*IRB*): In reference to a *research* project, a board that is designated to review and approve proposed *research*, and the process by which the investigator intends to secure the informed authorization of *research* subjects.

Limited Data Set: A set of identifiable healthcare information that the *HIPAA* Privacy Rule permits *covered entities* to share with certain entities for *research* purposes, public health activities, and healthcare operations without obtaining prior authorization from patients, if certain conditions are met including the exclusion of *HIPAA* specified direct identifiers of the *individual*, or of relatives, employers or household members of the *individual*.

Marketing: The provision of information about a product or service that encourages recipients of the communication to purchase or use the product or service. However, the *following items are excluded from the definition of marketing for purposes of this policy manual*:

a. Refill reminders or communications about a drug currently prescribed for the *individual* unless the *covered entity* sending it is reimbursed in excess of the cost of the communication;

b. unless the *covered entity* making the communication receives remuneration, communications for *treatment* and *health care operations* of the following types are not marketing: For *treatment* of an *individual* by a health care *provider*, including case management or care coordination for the *individual*, or to direct or recommend alternative *treatment*s, therapies, health care *providers*, or settings of care to the *individual*;

c) To describe a health-related product or service (or *payment* for such product or service) that is provided by, or included in a plan of benefits of, the *covered entity* making the communication, including communications about: the entities participating in a health care *provider* network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

d) For case management or care coordination, contacting of *individual*s with information about *treatment* alternatives, and related functions to the extent these activities do not fall within the definition of *treatment*.

Medical Record: documents, notes, forms, and test results that collectively document health and healthcare services for an *individual* including but not limited to medical history, care or *treatment*s received, medications prescribed or taken, test results, diagnosis and prognosis. *Psychotherapy notes* are excluded from the definition of *medical record* as are peer review documents when they are covered by a legal privilege.

Minimum Necessary Standard: use of reasonable efforts to limit the use or disclosure of *PHI* to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request

Notice of Privacy Practices: A document required by the *HIPAA* Privacy Rule. The Notice of Privacy Practices must provide *individual*s with information on how an organization will use or disclose their *PHI*, what the organization's responsibilities are and what *individual*s' rights are with respect to that *PHI*.

Office for Civil Rights (*OCR*): The branch within the Department of Health and Human Services that enforces *HIPAA*.

Opt-out: To make a choice to be excluded from communications or practices.

Payment. Activities undertaken by a health care *provider* or health plan to obtain or provide reimbursement for the provision of health care. Activities undertaken by a health plan to obtain premiums or to determine the full extent of its coverage and benefit provision under the health plan. Activities for *payment* include eligibility of coverage determination, billing, claims management, collection activities, medical necessity determinations, risk adjustments, utilization review including precertification, preauthorization, concurrent and retrospective review of services, and specified disclosures to consumer reporting agencies.

Personal representative is one who, under law, has the authority to act on behalf of an *individual* in making decisions related to health care or in exercising the *individual*'s rights related to their protected health information. *Personal representative*s' rights are limited in certain circumstances.

Privacy *Breach*: any unauthorized or unpermitted *access*, use, disclosure, modification, or destruction of *unsecured PHI* in any form.

Privacy incident: any attempted or successful unpermitted or unauthorized *access*, use, disclosure, modification, interference or destruction of *unsecured PHI* in any form.

Privacy Officer: **Organization's** designated *individual* who is responsible for overall compliance with the *HIPAA* Privacy Rule and for development and implementation of *HIPAA* policies and procedures.

Protected Health Information (*PHI*):
PHI is *individually identifiable health information* that is created, received, transmitted, or maintained by a *covered entity* or *business associate* in any form or medium. *PHI* excludes information regarding persons deceased for more than 50 years, information in education records (which are protected by other laws) and information in employment records held by a *covered entity* in its role as an employer. It includes genetic and demographic information.

Provider: A *provider* of medical or health services, and any other person or entity who furnishes, bills for, or is paid for health care in the normal course of business. *Providers* at the organization are those contracted, subcontracted, or employed who provide medical or health services on behalf of the organization.

Psychotherapy notes: Notes recorded in any medium by a mental health professional documenting or analyzing the contents of a conversation during a counseling session that are separated from the rest of the *medical record*. *Psychotherapy notes* do not include medication prescription and monitoring, session start and stop times, modalities and frequency of *treatment*, clinical test results, or summary information on diagnosis, functional status, *treatment* plan, symptoms, prognosis and progress to date.

Research: A systematic investigation designed to develop or contribute to generalized knowledge. *Research* is conducted through development, testing, and evaluation.

Security incident: a *HIPAA security incident* is an attempt (which can be successful or not) to do something unauthorized. The "something" that is unauthorized, is an unauthorized *access*, use, disclosure, modification, destruction, or interference with *ePHI*.

Treatment. The provision, coordination, or management of health care and related services, including the coordination or management of health care by a health care *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 health care *provider* to another.

Unsecured PHI: *PHI* that is not been rendered unusable, unreadable, or indecipherable to unauthorized *individual*s though the use of a technology or methodology specified by the *HHS* Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

Use: To share, employ, apply, utilize, examine, or analyze *individually identifiable health information*.

Whistleblower: An *individual* who reveals wrongdoing within an organization to the public, government agencies, or to those in positions of authority.

Workforce members: employees, volunteers, trainees, consultants, *providers*, professionals, managers, staff, and other persons whose conduct, in the performance of work for the **Organization**, is under the direct control of the **Organization**, regardless of whether these *individual*s are paid by the *covered entity*.

