HIPAA PRIVACY POLICY & PROCEDURE MANUAL

Prepared By: Jenna Lovaas & Kaci Ginn
May 27th 2020

HIPAA PRIVACY POLICY & PROCEDURE MANUAL

Jones County Iowa

Company Name: Will be referred as [Organization] throughout each policy.	**Jones County Iowa**
Policy Name:	Privacy Policy
Policy Version:	Version 1.0
Effective Date:	05/27/2020
Review Date:	Yearly
Security Officer: Will be referred as Security Officer throughout each policy.	Lisa Mootz
Privacy Officer: Will be referred as Privacy Officer throughout each policy.	Jenna Lovaas & Kaci Ginn
Compliance Officer: Will be referred as Compliance Officer throughout each policy.	Jenna Lovaas & Kaci Ginn
Responsible for Review:	Lisa Mootz/ Jenna Lovaas & Kaci Ginn

TABLE OF CONTENTS

Privacy Manual Synopsis

This section is for all employees to review and attest. Below is a summary of each policy, including the relevant HIPAA regulations. To view the full policy of a section, 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.

Privacy 1.0 HIPAA Privacy Program

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 of protected health information (PHI), maintain sensitive organization information, and prevent and detect inappropriate and illegal uses and disclosures of PHI. Employees must be familiar with the Privacy Officer's job functions, and must contact the Privacy Officer when this Policy requires that they do so.

§164.530 *HIPAA Privacy Program*

Privacy 2.0 Accounting of Disclosures

Individuals 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. Individuals can exercise this right by making a written request to **organization** for an accounting. **Organization** must properly respond to the request, and send the accounting when appropriate.

45 CFR § 164.528(a) *Accounting for Disclosures*

Privacy 3.0 Right to Amend

While the original PHI contained in a medical record cannot be altered, patients have the right to amend certain protected health information in their medical records. Amendment consists 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 individuals as to whether their request is granted or denied.

§ 164.526(a)(1) *Amendment of Protected Health Information*

Privacy 4.0 Business Associates

Organization relies on business associates, which are vendors that handle **organization** functions that require access to PHI. 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.

§ 164.502(e)(1) *Disclosures to Business Associates*
§ 164.504 *Uses and Disclosures: Organizational Requirements*

Privacy 5.0 Charging for Copies of PHI

Organization can charge individuals requesting copies of their PHI a cost-based, reasonable fee. Employees must understand how to respond to requests for copies of PHI, so patients are charged the proper amount, and are given the information they request in a timely fashion.

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

Privacy 6.0 Communication of PHI

Organization must safeguard and protect the privacy of PHI while using various means of communication (i.e., fax, phone, email, mail, mobile device) involving that PHI. Workforce members must understand what security measures are required for each of these types of communication.

45 CFR 164.306, 45 CFR 164.312(a)(2)(iv), 45 CFR 164.312(e)(2)(ii), 45 CFR 164.501,45 CFR 164.502, 45 CFR 164.508, 45 CFR 164.514 , 45 CFR 164.520, 45 CFR 164.522, 45 CFR 164.528, 45 CFR 164.530

Security Standards: General Rules, Encryption and Decryption, Encryption, Definitions, Uses and Disclosures of PHI: General Rules, Uses and Disclosures for Which an Authorization is Required, Other Requirements Relating to Uses and Disclosures of PHI, Notice of Privacy Practices for PHI, Rights to Request Privacy Protection for PHI, Accounting of Disclosures of PHI, Administrative Requirements.

Privacy 7.0 Fundraising and PHI

Organization may use and disclose individual PHI for certain fundraising purposes. In addition, **organization** must permit individuals the right to opt out of receiving fundraising communications, and to withdraw authorizations permitting such activities. The Notice of Privacy Practice shall contain provisions regarding the right to opt out and to revoke authorization.

45 CFR § 164.514(f)(1) & (f)(2) *Uses and disclosures for fundraising & Implementation specifications: Fundraising requirements*
45 CFR §164.501 *Definitions*

Privacy 8.0 Right to Request Privacy Protections for PHI

Organization will honor patient 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 individuals to receive communications of PHI by alternative means or at an alternate location. Workforce members shall be trained as to how to respond to all such requests.

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

Privacy 9.0 Identity Verification

Before **organization** discloses PHI to an individual or organization requesting it, organization must verify the identity of the individual or organization.

§164.514(h)(1) *Identity Verification Requirements*

Privacy 10.0 Judicial and Administrative Proceedings

Organization must disclose a patient's PHI when that PHI is sought in a judicial or administrative proceeding. Such proceedings include court proceedings, and proceedings before government agencies, such as the Department of Health and Human Services ("HHS") and the Centers for Medicare and Medicaid Services ("CMS"). Employees will be trained as to how to respond to requests for PHI sought in these proceedings.

§164.512(e) *Use and Disclosure of PHI for Judicial and Administrative Proceedings*

Privacy 11.0 Uses and Disclosures for Marketing

Organization may use or disclose PHI for certain marketing purposes. **Organization** may not use or disclose PHI for marketing activities that are purely commercial. Employees will be trained as to when PHI can be disclosed for marketing activities.

164.508 (a)(3) *Uses and Disclosures for Which an Authorization is Required: Marketing*

Privacy 12.0 Minimum Necessary

Under the minimum necessary standard, **organization** may only use, request, or disclose that PHI that is necessary to fulfill a request, or perform a job function. Employees will be trained on this standard so that PHI is used, requested, or disclosed only to the extent that is legally required.

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

Privacy 13.0 Minors' Rights

This policy covers when minors must access their PHI through a personal representative, and when minors may access their PHI directly. **Organization** employees must be familiar with the circumstances under which minors can access their PHI without parental or personal representative approval or knowledge.

164.502(g) *Personal Representatives*

Privacy 14.0 Patient Right to Access and Inspect Medical Records

Organization must afford patients the opportunity to access and inspect their medical records. This policy covers how employees must respond to request access and inspection of medical records.

§164.524(a) *Patient Right to Access, Inspect, and Copy Medical Records*

Privacy 15.0 Psychotherapy Notes

Organization may generally not disclose psychotherapy notes to requesting parties. Certain exceptions allow organization to release this information. This policy serves to train **organization** employees as to what constitutes psychotherapy notes, and when such notes may be used or disclosed.

§164.508(a) *Authorizations for uses and disclosures*

Privacy 16.0 Uses and Disclosures for Which an Authorization is Required

Under certain circumstances, written patient authorization is necessary prior to organization's use or disclosure of that patient's individual's PHI. Written patient authorization must be validly obtained. This policy describes when written authorization is required, and what constitutes a valid authorization.

§164.508 *Uses and Disclosures for Which an Authorization is Required*

Privacy 17.0 Uses and Disclosures, No Authorization Required

Under certain circumstances, **organization** may use and disclose PHI when neither authorization nor an opportunity for a patient to agree or object is required. This policy

informs employees of what those circumstances are, and what steps employees must take to fulfill requests for PHI.

§164.501 *Uses and Disclosures for Health Care Operations*
§164.512 *Consent or Authorization Not Required*

Privacy 18.0 Uses and Disclosures Requiring Patient Opportunity to Agree or Object

Under some circumstances, **organization** must provide a patient the opportunity to agree or object to disclosure of PHI. This policy covers how **organization** responds to such requests made when these circumstances apply.

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

Privacy 19.0 Uses and Disclosures of Workers Compensation Information

Organization may release certain health information to state workers compensation or workers compensation insurance programs without patient authorization or release. This policy describes the circumstances under which such disclosure is required, and how to make the disclosure.

§164.512 *Consent or Authorization Not Required*

Privacy 20.0 Breach Notification

Organization must report, and make efforts to remediate, breaches of unsecured PHI. This policy outlines **organization's** and workforce members' obligations to identify breaches, report breaches, and send notifications regarding breaches.

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

Privacy 21.0 Notice of Privacy Practices

Organization must provide patients with its Notice of Privacy Practices. This notice describes how patient PHI is to be used and disclosed under the Notice of Privacy Practice.

§164.520(b) *Content of Notice of Privacy Practices*

§164.520(c)(2) *Provision of Notice of Privacy Practices*

Privacy 22.0 Social Media

Employees 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.

Privacy 23.0 Complaints About Organization

Organization must have a complaint process, under which individuals 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.

45 CFR 164.530(d) *Complaints*

Privacy 24.0 Sanctions

Workforce members who violate **Organization's** privacy policy and procedures are subject to sanctions. Sanctions are disciplinary measures intended 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 should be consistent, and proportional with the severity of the offense.

45 CFR 164.530(e) *Sanctions*
45 CFR 164.530(f) *Mitigation*

Privacy 25.0 No Retaliation; No Waiver of Rights

Organization shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual who exercises his or her rights under the Privacy Rule, including the right to file a complaint about **Organization's** privacy policies, practices, and procedures. In addition, **Organization** shall not require any person to waive these rights as a condition of the provision of treatment or payment for healthcare.

45 CFR 164.530(g) *Refraining from Intimidating or Retaliatory Acts*
45 CFR 164.530(h) *Waiver of Rights*

Privacy 26.0 Uses and Disclosures for Treatment, Payment, and Healthcare Operations

Organization is not required to obtain written patient authorization to use or disclose PHI under certain circumstances. When **organization** uses or discloses PHI for purposes of treatment, payment, or healthcare operations, **organization** need not obtain such authorization, except for certain exceptions, and when required to do so by state law.

45 CFR 164.506 *Treatment, Payment, or Healthcare Operations*

Privacy 27.0 Sale of PHI

Organization will not engage in activities constituting the sale of patient PHI, unless prior written patient authorization is obtained. "Sale of PHI" is the indirect or direct receipt of remuneration, including non-financial benefits such as in-kind benefits, in exchange for patient PHI.

45 CFR 164.508(a)(4) *Sale of PHI*

Privacy 28.0 Policy for Disclosures by Whistleblowers and Workforce Member Crime Victims

Workforce members and business associates have the right to disclose PHI if they believe another workforce member or business associate has engaged in conduct that violates the HIPAA regulations, or **organization's** policies and procedures relate to those regulations. In addition, workforce members who are the victim of a crime may disclose PHI about the suspected perpetrator to law enforcement officials.

45 CFR 164.502(j) *Disclosures by Whistleblowers and Workforce Member Crime Victims*

Privacy 29.0 Use or Disclosure of PHI for Specialized Government Functions

Organization may use and disclose PHI without written patient 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; and
- Correctional institutions and other law enforcement custodial situations.

45 CFR 164.512(k) *Uses and Disclosures for Specialized Government Functions*

Privacy 30.0 Limited Data Set and Data Usage 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.

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

Continued on Next Page

Privacy 1.0 HIPAA Privacy Program

FULL POLICY LANGUAGE:

Policy Purpose:

At all times, **organization** shall have one individual identified and assigned to HIPAA Privacy responsibility. This individual is known as the HIPAA Privacy Officer.

Policy Description:

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:

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

Training:

- **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:
    - To each new member of the workforce within a reasonable period of time after the person joins the workforce.
    - 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.
    - **Organization** must document that the training has been provided.
- Questions concerning training or any aspect of training may be directed to the Privacy Officer.

Administrative 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. The Privacy Officer ultimately has responsibility for these tasks.

Complaints:
Organization must provide a process for individuals to make complaints concerning its privacy policies and procedures, and its compliance with those procedures. **Organization** must keep records of complaints and their resolution.

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 it applies. The Privacy Officer shall be responsible for the determination of appropriate sanctions. The Privacy Officer, in his or her discretion, may review the sanction decision at the request of an employee.

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.

No Retaliation:
Organization may not threaten, coerce, discriminate against, or take other retaliatory action against anyone who files a complaint, or who exercises a right to which they are entitled under the Privacy Rule.

Waiver of Rights:
Organization may not require any individual to waive his or her right to file a complaint with organization or HHS, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Policies and Procedures:
The policies and procedures to be developed 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. **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, whenever is later.

RELEVANT HIPAA REGULATIONS:

- §164.530 *HIPAA Privacy Program*

Continued on Next Page

Privacy 2.0 Accounting of Disclosures

FULL POLICY LANGUAGE:

Policy Purpose:

The purpose of this policy is to ensure patients can receive an accounting of disclosures of their protected health information.

Policy Description:

Under HIPAA, **organization** must give patients an accounting of disclosures of PHI it made, upon patient request.

Required Disclosures:

Types of disclosures that **organization** must include in responding to a request for an accounting include:

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

Required Tracking:

Information that must be maintained (tracked) and included in an accounting shall consist of:

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 (or a copy of the individual's written authorization) or a copy of the individual's written request for disclosure; and
5. Multiple disclosures to the same party for a single purpose (or pursuant to a single authorization) 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.

Disclosures Not to Be Included in an Accounting:
An accounting of disclosures shall not include the following disclosures:

1. Disclosures made to law enforcement or correctional institutions as provided by state law;
2. Disclosures for facility directories;
3. Disclosures to the individual patient;
4. Disclosures for national security or intelligence purposes;
5. Disclosures involved in the patient's care;
6. Disclosures made for notification purposes, including identifying and locating a family member; and
7. Disclosures made for treatment, payment, and healthcare operations.

Patients may request an accounting of disclosures that were made up to six years prior to the date of request.

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.
3. A patient 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 the third party, and maintain a record of the name/departments responsible for the completion of the accounting.

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 patient records that contain patient disclosures;
2. Obtaining a Patient Disclosure Report from all departments that maintain such reports;
3. Contacting business associates, as necessary, to request the information provided.

Preparing the Accounting of Disclosures:
Accountings of disclosures shall be prepared by **organization** as follows:

1. Each item on the accounting of disclosures to be sent to the patient must include:

- The date the disclosure was made;
- 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);
- A brief description of the PHI that was disclosed; and
- A brief description of the purpose of the disclosure.

2. Each disclosure made to an external researcher for a particular research purpose involving 50 or more individuals to an Institutional Review Board waiver of authorization must include:
    - The name of the protocol or other research activity;
    - 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;
    - A brief description of the types of PHI that were disclosed;
    - The date or period of time during which disclosures occurred;
    - The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
    - A statement that the PHI of the patient may or may not have been disclosed for a particular protocol or research activity.

Sending the Accounting:

1. In accordance with the HIPAA regulations, **organization** must provide the individual with an accounting no later than **60** days after receipt of the request.
2. If the accounting cannot be completed within 30 days after receipt of the request, **organization** must 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. The **organization** must 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.
4. **Organization** must provide the accounting to the individual at no charge for a request made once during any twelve-month period.
    - 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:

- **Organization** must maintain written requests for an accounting provided to an individual for at least six years from the date it was created.
- **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 C.F.R. § 164.528(a) *Accounting for Disclosures*

Continued on Next Page

Privacy 3.0 Right to Amend PHI

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. Under HIPAA, individuals have the right to request an amendment of protected health information contained in a designated record set.

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

Policy Description:

The HIPAA Privacy Rule grants individuals the right to amend or supplement their own protected health information, for as long as a covered entity (organization) maintains the PHI. The right to amend includes the right to correction of errors; the right to supplement an existing record with additional PHI. The protected health information patients can amend must be associated with the use, disclosure, and maintenance of their records in a designated record set. A designated record set is a group of records maintained by or for **organization,** which includes billing records, medical records, and other records **organization** uses to make decisions about patients.

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 amended, as well as the reasons for the amendment.

Responding to a Request for Amendment:

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. If **organization** approves the request for amendment, **organization** must timely inform the individual that the request to amend has been accepted, and make the appropriate amendment.

If **the request is granted,** after review and approval by the individual responsible for the entry to be amended, **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 which 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 if **organization** determines that the information or record:

- Was not created by **organization**, unless the originator of the protected health information is no longer available to make the amendment;
- Is not part of a designated record set;
- Would not be available for inspection (under the Privacy Rule "right of access" standard, individuals may both view their PHI as well as have copies made of that PHI);
- Is accurate and complete.

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

- The basis for the denial;
- The individual's right to submit a written statement disagreeing with the denial and how to exercise that right;
- 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); and
- A description of how the individual can file a complaint with **organization** or the Secretary of the Department of Health and Human Services (HHS).

Organization must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by the HIPAA Privacy Rule.

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 Amendments:
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 amendments.

Participation of Uninvolved Third Parties:
It may be determined that a further review of the patient's request for amendment requires 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 and medical staff leadership.

Additional Considerations of Amendments from Other Covered Entities:
When **organization** receives notification from another covered entity that an individual's protected health information has been amended, **organization**:

- Must ensure that the amendment is appended to the individual's designated record; and
- Will inform its business associates, that may use or rely on the individual's designated record set, of the amendment (as agreed to in the business associate contract), so that they may make the necessary revisions based on the amendment.

RELEVANT HIPAA REGULATIONS:

- § 164.526(a)(1) *Amendment of Protected Health Information*

Privacy 4.0 Business Associates

FULL POLICY LANGUAGE:

Policy Purpose:

The purpose of this policy is to provide rules for **organization's** determining whether a vendor is a business associate as defined by the HIPAA regulations. The purpose is also to provide rules for creation, maintenance, and termination of business associate agreements.

Policy Description:

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, use, or disclosure of protected health information. 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 receives, uses, or discloses in carrying out specified functions or activities for a covered entity. **Organization** may only disclose protected health information (PHI) to a business associate after a valid business associate agreement is in place.

Procedures:

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 on behalf of the **organization**;
- That "something" involves the access to, use, and/or disclosure of PHI.

To make the business associate determination, **organization** will inventory all outside business and service vendors to determine if they are business associates.

Business associate agreements shall be implemented for all qualified entities. These agreements shall require that business associates comply with the minimum necessary standard set forth in 45 C.F.R. 164.502(b). Under this standard, business associates must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the PHI use, disclosure, or request.

Business Associate Contracts/Agreements:

If an entity is determined to be a business associate, that business associate must provide in writing to **organization** 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 shall be in the form of a written business associate contract (BAC) that contains the provisions specified in the Privacy Rule. These provisions must:

1. Establish the permitted and required uses and disclosures of protected health information by the business associate;
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 with regard to electronic protected health information;
4. Require the business associate to report to **organization** any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information;
5. Require the business associate to disclose protected health information as specified in its contract to satisfy **organization's** obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings;
6. 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 applicable to the obligation;
7. 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;
8. 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;**
9. Require the business associate to ensure that any subcontractors it may engage on its behalf, that will have access to protected health information, agree to the same restrictions and conditions that apply to the business associate with respect to such information; and
10. Authorize termination of the contract by the **organization** if the business associate violates a material term of the contract.

In the Event of Material Breach or Violation:
If **organization** knows of a material breach or violation by the business associate of the contract or agreement, the **organization** is required to take reasonable steps to cure the breach or end the violation.

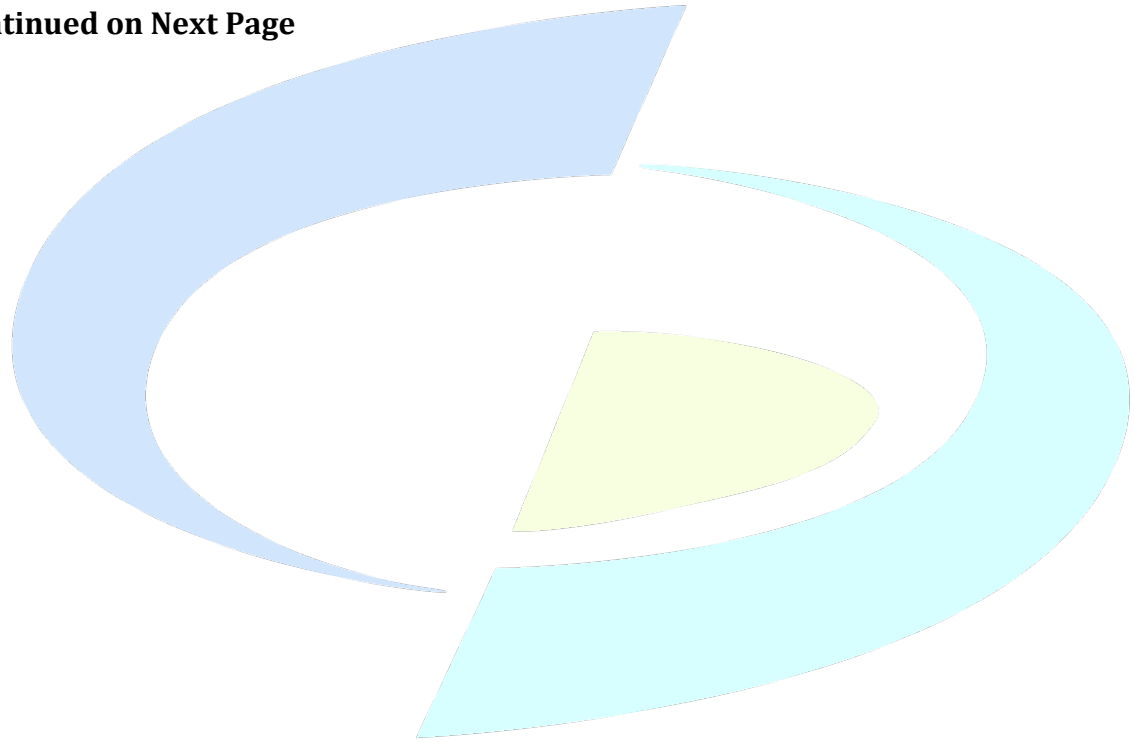
If such steps are unsuccessful, the **organization** must terminate the contract or agreement. If termination of the contract or agreement is not feasible, the **organization** must report the problem to the Secretary of the Department of Health and Human Services (HHS).

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

RELEVANT HIPAA REGULATIONS:

- § 164.502(e)(1) *Disclosures to Business Associates*
- § 164.504 *Uses and Disclosures: Organizational Requirements*

Continued on Next Page



Privacy 5.0 Fees for Copies of PHI

FULL POLICY LANGUAGE:

Policy Purpose:

To detail the regulations regarding what fees **organization** can charge patients for requests of copies of their PHI.

Policy Description:

The HIPAA Privacy Rule authorizes **organization** to impose reasonable, cost-based fees for responding to requests made by an individual (patient or legal representative) for copies of PHI for their own, personal use. Under the Privacy Rule, fees may only be charged for the costs of copying, including the labor and supply costs. For example, if hard copies are made, the **organization** may charge for the costs of paper. If electronic copies are made to a CD, the **organization** may charge a fee for the cost of the CD.

If the patient has agreed to receive a summary or explanation of his or her PHI, **organization** may charge a fee for preparation of the summary or explanation. This fee may not include costs associated with searching for and retrieving the requested information. As a courtesy, **organization** may, in its discretion, waive copy charges for the disclosure of PHI between providers.

Procedures:

Processing Requests:

- **Organization** must produce records requested by a patient for their individual use within **30 days** from the date of request.
- Patient is entitled to access those records that are in one or more designated record sets.
- If **organization** requires an extension of time, **organization**, per HIPAA requirements, can take an additional 30 days to provide the information, provided **organization**, within the initial 30-day period, provides written notice to the patient stating the reason for the delay and the expected date of production.
- The **organization** may not charge fees for the retrieval, handling, or processing of request for PHI requests made by a patient for their personal use.
- If an individual requests that the information be mailed, the individual is entitled to a mailing. **Organization's** fee may include the cost of postage.
- If an individual asks for an explanation or summary of the information provided, and agrees in advance to any associated fees, **organization** may, after notifying patient, charge for preparing the explanation or summary.
- If an individual requests an "accounting of disclosures" to identify what PHI has been disclosed to others, **organization** must provide the first accounting free in any 12-month period. Subsequent requests made during the 12-month period can include a reasonable fee based on costs to the **organization** for providing an

accounting. Before charging the fee, the **organization** must inform the patient and allow them the opportunity to withdraw or modify the request to avoid or reduce the fee.

Specific Instances Where Fee is Not Permitted:
Organization may not charge fees for 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.

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. As such, a State law fee may be considered excessive under the HIPAA "reasonable, cost-based fee" standard. When a State law conflicts with HIPAA on this matter, HIPAA prevails.

Organization shall not charge a fee for providing, releasing, or delivering medical records or copies of medical records, 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 patients' request.

Flat Fee for Requests for Electronic Copies of PHI:
Organization, in its discretion, may charge individuals 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.

RELEVANT HIPAA REGULATIONS:

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

Continued on Next Page

Privacy 6.0 Communication 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 via the communication media listed. PHI shall be disclosed to personnel, patients, their personal representatives, other covered entities, public health officials, and business associates, in accordance with HIPAA regulations and this policy.

Policy Description:

PHI can be communicated through various media, including mail, facsimile, and electronically. PHI must be safeguarded from unauthorized access during the communication process. The HIPAA Privacy Rule section 164.530 (c)(1) requires **organization** to develop and implement safeguards to protect the privacy of PHI. 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.

Procedures:

Methods of Transmission:

PHI may be transmitted through several media. These include:

- Oral media (conversations, telephone, cell phone, answering machines, announcements)
- Mail (both within the organization, and between the organization and a third party)
- Fax
- Email

Orally Communicating PHI:

Privacy regulations are not intended to prohibit providers from speaking to each other and to their patients; however, CEs/BAs are required to implement reasonable safeguards that reflect their specific circumstances. Sometimes healthcare providers will incidentally disclose PHI to perform their duties. For example, in a busy emergency room, it may be necessary for providers to speak loudly to ensure the correct treatment. The following practices are acceptable, if reasonable precautions are taken to minimize the chance of unintentional disclosures to others who may be nearby (such as using lowered voices or talking away from others):

- Health care staff may orally coordinate services at hospital nursing stations.
- Nurses or other health care professionals may discuss a patient's condition over the phone with the patient, a provider, or a family member.

- A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.
- A physician may discuss a patient's condition or treatment program in the patient's semiprivate room.
- Health care professionals may discuss a patient's condition during training rounds in an academic or training institution.
- A pharmacist may discuss a prescription with a patient over the pharmacy counter or with a physician or the patient over the phone.

Reasonable precautions **organization** should consider implementing include:

- Providers should speak quietly and avoid using patients' names in a waiting room, public hallways, elevators, and any other public areas.
- Providers could add curtains or screens to areas where oral communication often occurs between doctors and patients or among professionals treating the patient.
- In an area where multiple patient-staff communication routinely occurs, use of cubicles, dividers, shields, or similar barriers may constitute a reasonable safeguard.

Mailing PHI:
Transmitting paper or other tangible PHI by US Mail or reliable delivery services such as UPS, FedEx, and DHL are permissible, but **organization's** workforce should use common sense in not overstuffing envelopes, and use appropriate boxes and envelopes to minimize the possibility of loss in transit. Mailings to patients may include the name and address of the patient but should not include additional information about the patient.

Transmission Through Fax:
1. Fax PHI only when other types of communication are not available or practical.
2. Limit the PHI contained in the fax to the minimum necessary to accomplish the purpose of the communication.
3. When faxing to a patient, do not fax sensitive PHI such as PHI related to alcohol abuse, drug abuse, mental health issues, HIV testing, antigens indicating hepatitis infection, sexually transmitted diseases (STD), or presence of malignancy.
4. Do not use faxing as a means to respond to subpoenas, court orders, or search warrants.
5. Take reasonable precautions to ensure that the intended recipient is either available to receive the fax as it arrives or has exclusive access to the fax machine.
6. Pre-program frequently used, non-patient fax numbers, to minimize potential for misdirected faxes. Confirm pre-programmed numbers at least every six (6) months.
7. If there is any reason to question the accuracy of a fax number, contact the recipient to confirm the number prior to faxing PHI.
8. When faxing PHI, use 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

9. Accompany the fax with a confidentiality notice. The following language may be used: "The information contained in this facsimile transmission is privileged and confidential intended for the use of the addressee listed on the cover page. The authorized recipient of this information is prohibited from disclosing this information to any other party and is required to destroy the information after its stated need has been fulfilled. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited (Federal Regulation 42 CFR, Part 2, and 45 CFR, Part 160). If you have received this fax in error, please notify the sender immediately by calling the phone number above to arrange for return of these documents."
10. Do not include any PHI on the fax cover sheet.
11. If notified of a misdirected fax, instruct the unintended recipient to return the information by mail or destroy the information by shredding.

Emailing PHI:
Organization should take certain precautions when using email to avoid unintentional disclosures. These include:

1. Checking the email address for accuracy before sending, and sending an email alert to the patient for address confirmation prior to sending the message.
2. Encrypting treatment-related communications.
3. **Organization** should not use email for sensitive or urgent matters. Email should be used for appointment scheduling and routine follow-up questions.
4. Do not use email to convey the results of tests related to HIV status, sexually transmitted diseases, presence of a malignancy, presence of a hepatitis infection, or abusing the use of drugs.
5. Limit the PHI contained in the email to the minimum necessary to accomplish the purpose of the communication.
6. Email PHI only to a known party (i.e., patient, health care provider).
7. Prior to emailing PHI to an individual:
    - Obtain the individual's consent to communicate PHI with him or her even if the individual initiated the correspondence; and
    - Clearly communicate to the individual the risks and limitations associated with using email for communications of PHI.
8. When emailing to a non-healthcare provider third party, always obtain the consent of the individual who is the subject of the PHI.
9. Do not email PHI to a group distribution list unless all individuals have consented to such method of communication.

10. Send PHI as a password-protected/encrypted attachment.
11. In the subject heading, do not use patient names, identifiers or other specifics; consider the use of a confidentiality banner such as "This is a confidential medical communication."
12. Include in the email a confidentiality notice, such as the following: "Confidentiality Notice: This email transmission, and any documents, files or previous email messages attached to it, may contain confidential information. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution, or use of any of the information contained in or attached to this message is STRICTLY PROHIBITED. If you have received this transmission in error, please immediately notify us by replying to the email or by telephone at (XXX) XXX-XXXX, and destroy the original transmission and its attachments without reading or saving them to disk."

Storage and Disposal of PHI:

1. Maintain documents containing PHI in locked cabinets or locked rooms when the documents are not in use and after working hours.
2. Establish physical and/or procedural controls (i.e., key or combination access, access authorization levels) that limit access to only those persons who have a need for the information.
3. Control and secure keys to locked files and areas. Do not leave keys in locks or in areas accessible to persons who do not have need for the stored PHI.
4. Do not place documents containing PHI in trash bins. Promptly shred documents containing PHI when no longer needed.

RELEVANT HIPAA REGULATIONS:

- 45 CFR 164.306 *Security Standards: General Rules*
- 45 CFR 164.312(a)(2)(iv) *Encryption and Decryption*
- 45 CFR 164.312(e)(2)(ii) *Encryption*
- 45 CFR 164.501 *Definitions*
- 45 CFR 164.502 *Uses and Disclosures of PHI: General Rules*
- 45 CFR 164.508 *Uses and Disclosures for Which an Authorization is Required*
- 45 CFR 164.514 *Other Requirements Relating to Uses and Disclosures of PHI*
- 45 CFR 164.520 *Notice of Privacy Practices for PHI*
- 45 CFR 164.522 *Rights to Request Privacy Protection for PHI*
- 45 CFR 164.528 *Accounting of Disclosures of PHI*
- 45 CFR 164.530 *Administrative Requirements*

Privacy 7.0 Fundraising and PHI

FULL POLICY LANGUAGE:

Policy Purpose:

To ensure **organization's** fundraising activities are conducted consistently with the Privacy Rule.

Policy Description:

Fundraising activities that contain only demographic information and dates of service may be conducted by **organization** for its benefit, without written patient authorization. Fundraising activities that disclose more than demographic information and dates of service require written patient authorization. All fundraising materials must describe how an individual can opt out of receiving future fundraising communications. **Organization** must make reasonable efforts to comply with opt-out requests.

Procedures:

1. **Organization**, when fundraising for its own benefit, may use or disclose, without written patient 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; and
   b. Dates of healthcare provided to an individual.
2. **Organization's** Notice of Privacy Practices must include the following information:
   a. **Organization** or 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. The communication must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications 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. If the fundraising is not for the **organization's** benefit, or includes more than demographic or dates of service information, a written authorization from the individual is required.

Opting-Out Procedures:

1. **Organization** must make reasonable efforts to ensure that individuals 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 will maintain a log of all patients 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 patient's fundraising authorization has been revoked, the **organization** may not send additional fundraising communications to the patient.

RELEVANT HIPAA REGULATIONS:

- 45 CFR § 164.514(f)(1) & (f)(2) *Uses and disclosures for fundraising & Implementation specifications: Fundraising requirements*
- 45 CFR §164.501 *Definitions*

Continued on Next Page

Privacy 8.0 Right to Request Privacy Protections for PHI

FULL POLICY LANGUAGE:

Policy Purpose:

This policy covers how **organization** must honor patient 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:

Patients have the right to request restrictions on how and where their PHI is communicated.

Patients may, in writing, request restrictions on:

- The use and disclosure of PHI for treatment, payment, or healthcare operations; or
- The disclosures to family, friends, or others for involvement in care and notification purposes.

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

Procedures:

Response to Request for Restriction:

1. Patients shall be notified of the right to request restrictions on the use and disclosure of PHI in **organization's** Notice of Privacy Practices, and that the request must be in writing.
2. The Privacy Officer shall manage requests for restrictions. All documentation associated with the request shall be placed in the patient's medical record.
3. The Privacy Officer shall provide a patient with a *Request to Restrict Use and Disclosure of Protected Health Information* form ("Request to Restrict" form) if a patient asks to make a restriction.
4. The patient must complete and sign the form. The Privacy Officer and/or his or her designated representatives may assist the patient in completing the form, if necessary.
5. Once the request has been completed, the Privacy Officer shall review the request, in consultation with other **organization** staff, to determine the feasibility of the request. The **organization** shall give primary consideration to the patient's need for access to the PHI for treatment and payment purposes in making its determination.
6. The Privacy Officer shall provide a written response to the request, and give a copy of that response to the patient.
7. If **organization** refuses the request, the Privacy Officer must provide the patient with a written copy of the refusal.

Restrictions on Accepted Requests:

1. If **organization** accepts the requested restriction, **organization** must abide by the terms of that restriction, with the following exceptions:
    - **Organization** may use the restricted PHI, or may disclose such information to a healthcare provider, *if* (1) the resident 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.
    - **Organization** may disclose the information to the patient who requested the restriction.
    - **Organization** may use and disclose information contained in its Facility Directory, unless patient has objected to such use.
    - **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 shall notify appropriate staff of the restriction.
3. The Privacy Officer shall 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.

Termination of Restriction with Patient's Agreement:

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

Termination of Restriction Without Patient's Agreement:

1. **Organization** may terminate the restriction without the patient's agreement if the **organization** informs the patient that the restriction is being terminated.
2. Such termination shall only be effective with respect to PHI created or received after **organization** has informed the resident 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 patient of the restriction.
3. If **organization** informs the patient by mail that it is terminating the restriction, the organization shall send the notification via certified mail, return receipt requested. **Organization** shall maintain a copy of the notification and the return receipt. **Organization** may only terminate the restriction upon confirmation that patient has received the notification.

4. If **organization** informs the patient in person that it is terminating the restriction, **organization** shall ensure that the patient signs and dates the notification of termination. **Organization** may alternatively document that the resident was notified on the *Request to Restrict* form.
5. If **organization** informs the patient by telephone, the **organization** shall document this action. In addition, **organization** shall send a letter to the patient via certified mail, return receipt requested. **Organization** shall deem such termination to be effective as of the date it informs the resident by telephone.

In addition, patients may also request communication of PHI by alternative means or at an alternate location. **Organization** shall accept 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 21).
2. **Organization's** Privacy Officer shall oversee and manage requests to receive communications by alternative means.
3. **Organization** may require a patient to make the request for communication by alternative means or at alternate location in writing.
4. When an inquiry is received from a patient regarding the right to request that the **organization** communicate with him or her, or his or her personal representative, by some alternate means, **organization** shall provide patient with a copy of 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 patient or the patient's personal representative.
5. The **Organization** may require that requests contain a statement that disclosure of PHI could endanger the patient. (The statement could be oral or written. Staff could ask patients if disclosure of PHI could put them in danger, or patients could fill out a request form that contains a checkbox question about possible endangerment due to PHI disclosure).
6. The Privacy Officer shall review the completed *Request for Communications* form to determine if the request is reasonable. **Organization** may not require an explanation for the request. **Organization** may not base its decision on the perceived merits (i.e., whether patient has a "good reason" for making the request) of the request. **Organization** will accommodate a request that it determines is reasonable (administratively feasible). **Organization** should create policies and procedures to determine the criteria for "reasonableness."
7. The Privacy Officer will complete the Response section of the Request for Communications form to inform the patient of the **organization's** decision.
8. If the **Organization** grants a patient'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 patient's medical record.

RELEVANT HIPAA REGULATIONS:

- §164.502(c) *Uses and Disclosures of PHI Subject to an Agreed Upon Restriction*
- §164.502(h) *Confidential Communications*
- §164.522 *Rights to Request Privacy Protection for PHI*

Continued on Next Page

Privacy 9.0 Identity Verification

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. 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, prior to a disclosure.

Procedures:

Organization will verify the identity and confirm the authority of any individual outside of **organization** requesting PHI.

When the Requester is the Patient:

When the requester is the patient, 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 patient's record.

When the Requester is the Patient's Personal Representative:

When the Requester is the patient'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 person's personal representative.

If there is no person listed in the medical record as the patient'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 of the person (or guardian ad litem) of the patient.

When the Requester is a Public Official or Law Office:

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 request on government letterhead.
3. 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, must immediately alert their supervisor. The supervisor shall then forward the request to a Designated Official(s) of the organization, The Designated Official, and that person alone, may respond to the request.

[List name of Designated Officials here. The Designated Officials may be the Privacy Officer, Compliance Officer, or Legal Counsel].

If the public official's request is an administrative request, subpoena, or a request related to an investigation, the Designated Official 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 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.

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 who is not known or recognized presents a written authorization by the patient as the basis for obtaining PHI, workforce members shall request that the person present photo identification to verify that the individual is indeed the person named in the authorization to receive the PHI.

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 Designated Official for guidance.

RELEVANT HIPAA REGULATIONS:

- §164.514(h)(1) *Identity Verification Requirements*

Continued on Next Page

Privacy 10.0 Judicial and Administrative Proceedings

FULL POLICY LANGUAGE:

Policy Purpose:

To establish rules for how **organization** shall respond to requests for disclosure of PHI in the course of judicial or administrative proceedings.

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. **Organization** must cooperate with courts and with counsel to provide lawfully sought PHI, while simultaneously ensuring protection of patient privacy.

Procedures:

Disclosing PHI in Response to a Court/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 the disclosure of.

The Privacy Officer, working with legal counsel, shall review any such order to determine whether **organization** will object to the order on account of over breadth, irrelevance, or any other lawful basis for objecting to disclosure. If the Privacy Officer and legal counsel conclude that an objection to the order is required, such objection shall be filed in accordance with applicable state 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:
   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.
   a. "Satisfactory assurance" that the requesting party has tried to notify the patient of the PHI includes the following:
      i. The requesting party has given the **Organization** a *written statement and supporting documentation* demonstrating that:
         1. The requesting party has made a good faith attempt to provide written notice to the patient (if the patient's location is unknown, documentation showing that a notice was mailed to the patient's last known address shall be provided by the requesting party);

2. The notice provided by the requesting party to the patient contained enough information to allow the patient to make an informed objection to the court or administrative tribunal regarding the release of the patient's PHI; and
3. The time for the patient to raise objections to the court or administrative tribunal has passed, and, either no objections were filed, **or,** all objections filed by the patient 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:
        i. 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
        ii. The requesting party has asked for a qualified protective order from such court or administrative tribunal.
3. 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 patient about releasing his or her PHI, so long as the notice meets all of the following requirements:
        i. The notice is written and given to the patient (if the patient's location is unknown, **Organization** should establish documentation showing that a notice was mailed to the patient's last known address);
        ii. The notice contained enough information to allow the patient to make an informed objection to the court or administrative tribunal regarding the release of the patient's PHI; and
        iii. The time for the patient to raise objections to the court or administrative tribunal has lapsed and either no objections were filed, or all objections filed by the patient 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 convince the parties to stipulate to such order.

RELEVANT HIPAA REGULATIONS:

- §164.512(e) *Use and Disclosure of PHI for Judicial and Administrative Proceedings*

Continued on Next Page

Privacy 11.0 Uses and Disclosures for Marketing

FULL POLICY LANGUAGE:

Policy Purpose:

To establish rules for how **organization** shall utilize PHI for marketing purposes.

Policy Description:

Organization engages in marketing activities. These activities are defined as communications about products and services that encourage recipients of the communication to buy or use those products and services. Generally, marketing that seeks to utilize protected health information require prior written patient authorization.

Procedures:

Determine Whether the Communication is Marketing:

1. Per §164.501, marketing is defined as:
   a. Making a communication about a product or service that encourages the recipients of the communication to purchase or use the product or service; or
   b. An arrangement involving **organization** and another entity or affiliate, whereby PHI is disclosed by **organization**, in exchange for direct or indirect remuneration, so that the other entity or affiliate can make a communication that encourages the purchase or use of its own product or service.
2. The following are examples of situations that **do not** meet the definition of marketing:
   a. Communications that are merely promoting good health, that are not related to a specific product or service, are not considered "marketing." Examples include information about how to lower cholesterol; mailings about general new developments in healthcare; new diagnostic tools; and mailings about upcoming health or "wellness" classes, support groups, and health fairs.
   b. Communications about government-sponsored programs. Under the Privacy Rule, there is no "commercial" component to communications about benefits available through public programs. Therefore, **organization** is permitted to use/disclose PHI to communicate about, for example, eligibility for Medicare supplement benefits; such communication does not require prior written patient authorization.
   c. The **organization** may make communications in newsletter format without authorization so long as the content of such does not fit the definition of "marketing," above.
   d. Oral or written communications that describe the **Organization's** network or covered services:
      i. The **Organization** can convey information to beneficiaries and members about health insurance products offered by the **Organization** that could enhance or substitute for existing health plan coverage. For example, if a child is about to "age-out" of coverage under a family's policy, the plan may

send the family information about continuation coverage for the child; this information is not considered "marketing." However, if the communication contains information about excepted benefits, such as accident-only policies or to other lines of insurance, the communication is considered to be marketing.

e. Communications about treatment for the patient; Doctors can write a prescription or refer an individual to a specialist for follow-up tests because these are communications about treatment.
f. Communications about case management or care coordination, or recommendations of treatment alternatives and care options, including health care providers or settings of care.

Authorization to Use or Disclose PHI for Marketing Purposes:

1. The **Organization** shall obtain written patient 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 patient; or
   b. A promotional gift of nominal value provided by the **Organization**.
2. If the marketing involves the **organization's** receiving direct or indirect remuneration by a third party, written patient authorization is required. Such authorization shall state that such remuneration is involved.

RELEVANT HIPAA REGULATIONS:

- 164.508 (a)(3) *Uses and Disclosures for Which an Authorization is Required: Marketing*

Continued on Next Page

Privacy 12.0 Minimum Necessary

FULL POLICY LANGUAGE:

Policy Purpose:

To establish rules for ensuring PHI is only used and disclosed as needed.

Policy Description:

The HIPAA Privacy Rule generally requires covered entities, including **organization**, to adhere to a "minimum necessary" standard with respect to the use and disclosure of PHI. When using or disclosing PHI, **organization** shall make reasonable efforts to limit PHI uses, disclosures, and requests disclosed to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Procedures:

Applicability of Standard:

Generally, the minimum necessary standard applies:

To uses and disclosures of PHI that are permitted under the HIPAA Privacy Rule. The standard also applies:

- To the accessing of PHI or electronic protected health information (ePHI), **by**
- Covered entities, **to**
- Business associates and other covered entities.

In addition, the HIPAA minimum necessary standard applies to *requests* for PHI from other covered entities.

The minimum necessary requirement **does not apply** to:

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 patient information (with possible exception of psychotherapy notes);
3. Uses or disclosures made pursuant to a valid and HIPAA compliant authorization;
4. Disclosures requested by the individual or the individual's legal representative;
5. 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
6. Uses and disclosures that are required by 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 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. An individual's access will be controlled via ID and password. The sharing of logon IDs and passwords is prohibited.

Routine or Recurring Requests and Disclosures for Patient Information:

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

Non-Routine Requests for Disclosure of Patient Information:

1. Non-routine requests for patient information will be reviewed 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. Such requests will be reviewed on an individual basis unless the request/disclosure is to a health care provider for treatment purposes.
3. Disclosures/requests authorized by the patient or the patient's legal representative will not be subject to the minimum necessary standard but are subject to 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 patient information reasonably necessary for the stated purpose, when:
    a. Making permitted disclosures to public officials, if the public official presents that the patient information is the minimum necessary for the stated purpose(s);
    b. The patient information is requested by another covered entity (i.e., health care provider, health plan or health care clearinghouse);

c. The patient information requested is the minimum necessary for the stated purpose and requested by a professional who is requesting patient information for the purpose of providing professional services to **organization** (i.e., member of **organization's** workforce or business associate of workforce); or
d. The documentation or representations comply with the applicable provisions for using/disclosing patient information for research purposes and have been provided by a person requesting the patient information for such purposes (i.e., appropriate documentation from the Institutional Review Board).

2. **Organization** workforce members should exercise judgment/discretion when making determinations about disclosures and limit the disclosure to the amount of patient information necessary to satisfy the purpose of the request.

Restrictions:

1. Use/disclosure of patient information will be subject to any agreed upon patient restriction(s) entered into by **organization** with the patient or the patient's legal representative.
2. Requests for restrictions that have been agreed to by **organization** should be placed in a designated area of the medical record. This area should be checked for restrictions prior to using/disclosing patient information.
3. Patient information may not be used/disclosed without proper consent or authorization.

Requesting Patient Information:

When requesting patient information from covered entities, **organization** will limit any request for patient information to that which is reasonably necessary to accomplish the purpose for which the request is made.

Corrective Action:

Upon determination of inappropriate or unauthorized access to PHI by a staff member, the **Organization** must determine the appropriate corrective action for the misconduct. Please refer to Privacy Policy 1 regarding failure to comply with privacy practices.

RELEVANT HIPAA REGULATIONS:

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

Privacy 13.0 Minors' Rights

FULL POLICY LANGUAGE:

Policy Purpose:

To provide minors access to their PHI when required by law.

Policy Description:

This policy 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:

To Whom Can Minors' PHI be Released?

Generally, a parent or guardian of a minor child is regarded as what the HIPAA Privacy Rule calls the "personal representative" of the minor child. Per the HIPAA Privacy Rule, a personal representative is authorized to exercise the HIPAA rights of the individual whom he or she represents, on that person's behalf. Therefore, a parent who is a personal representative can exercise a minor's HIPAA Privacy Rule rights with respect to protected health information (PHI), consistently with state law. In addition, personal representatives have the right to exercise other HIPAA Privacy Rule rights, such as providing written authorization for disclosure of PHI. The HIPAA Privacy Rule also gives a personal representative the general right to make medical decisions on the minor's behalf.

When is a Parent Not a Personal Representative?

The HIPAA Privacy Rule specifies *three* circumstances under which the parent is not the "personal representative" with respect to certain health information about his or her minor child.

These exceptions generally track the ability of certain minors to obtain specified health care without parental consent under state law, or standards of professional practice.

In these situations, the parent *does not* control the minor's health care decisions, and therefore under the HIPAA Privacy Rule, does not control the protected health information (PHI) related to that care. The three circumstances when a parent is not the minor's personal representative are:

- When state or other law does not require the consent of a parent or other person before a minor can obtain a particular health care service, *and* the minor consents to the health care service.
    - *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.

- When someone other than the parent is authorized by law to consent to the provision of a particular health service to a minor and provides such consent.
    - *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.
- When a parent agrees to a confidential relationship between the minor and a health care provider.
    - *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 Law Play?
The HIPAA Privacy Rule does not contravene state 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. If state law allows access, the HIPAA Privacy Rule does.

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 law. If state law prohibits disclosure, HIPAA does as well.

Can Organization Refuse to Regard a Person as a Personal Representative?
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*.

For example, if a physician reasonably believes that providing the personal representative of an incompetent elderly individual with access to the individual's health information would endanger that individual, the HIPAA Privacy Rule permits the physician to decline to provide such access.

RELEVANT HIPAA REGULATIONS:

- 164.502(g) *Personal Representatives*

Privacy 14.0 Patient Right to Access, Inspect, and Copy Medical Records

FULL POLICY LANGUAGE:

Policy Purpose:

It is the policy of the **Organization** to honor a patient's right to access, inspect, and obtain a copy of their PHI.

Policy Description:

This policy describes **organization's** procedures for ensuring patients' rights to access and inspect their protected health information.

Procedures:

Accessing and Inspecting PHI:

1. A patient must make a request to a staff member to access and inspect their PHI. Whenever possible, this request shall be made in writing and documented on either the "Authorization for Disclosure" form or in the notes of the patient's health record.
2. When access is granted, the **Organization** will provide visual access to the requested PHI within ten (10) days and furnish a copy within a reasonable time. If space is not available for visual inspection, the **Organization** must provide a copy within ten (10) days.
3. The **Organization** must document and retain the Designated Record Sets 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.

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

1. The patient and the **Organization** will arrange a mutually convenient time and place for the patient to inspect and/or obtain a copy of the requested PHI. Inspection and/or copying of PHI 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 as agreed to by the **Organization** and the patient.
    a. If the patient 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 patient chooses to copy their own information, the **Organization** may supervise the process to ensure that the integrity of the patient record is maintained.

3. Upon prior approval by the patient, the **Organization** may provide a summary of the requested PHI.
4. The **Organization** may charge a reasonable fee for the production of copies or a summary of PHI (please see Privacy Policy 5.0 for specifics).
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 3.0.

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

- The **Organization** will deny access to PHI if it contains:
    - Psychotherapy notes; or
    - Information complied in reasonable anticipation of, or for use in, civil, criminal, or administrative action or proceeding.

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

- The **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 patient, other inmates, or any other person.
- 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.
- PHI was obtained from someone other than a healthcare provider under promise of confidentiality and giving access would reveal the source of the information.
- An individual's access to PHI that is contained in records that are subject to the Privacy Act may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

Reviewable Denials:

The **organization** may deny access, provided the patient is given the right to have the denial reviewed, upon patient request, in the following circumstances:

- A licensed healthcare professional has determined that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person.
- 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.

- If it is determined that the request to review all or part of the patient information can reasonably be expected to cause substantial and identifiable harm to the subject or others which would outweigh the qualified person's right of access to the information.

Form of Denial:

Denials Must be in Writing:

The **Organization** must provide a written denial to the patient. The denial must be in plain language and must contain:

- The basis for the denial;
- A statement, if applicable, of the patient's review rights; and
- A description of how the patient may complain to the Organization or to the Secretary of Health and Human Services (HHS).

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 patient where to direct the request for access.
2. The **Organization** must, to the extent possible, give the patient access to any other PHI requested, after excluding the PHI as to which the **Organization** has grounds to deny access.
3. If access is denied under a situation where that denial may be reviewed, individual has the right to have the denial reviewed by a licensed health care professional who is designated by the **Organization** to act as a reviewing official and who did not participate in the original decision to deny.
4. 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.
5. The **Organization** must promptly provide written notice to the patient of the determination of the reviewing professional.

RELEVANT HIPAA REGULATIONS:

- §164.524(a) *Patient Right to Access, Inspect, and Copy Medical Records*

Privacy 15.0 Psychotherapy Notes

FULL POLICY LANGUAGE:

Policy Purpose:

To ensure workforce members understand what psychotherapy notes are, and to ensure workforce members understand when and how they can release psychotherapy notes and mental health treatment records to requesting parties.

Policy Description:

This policy describes how **organization** is to respond to requests for psychotherapy notes. Psychotherapy notes are defined under HIPAA as notes recorded in any medium by a mental health professional, and include the documenting or analyzing the contents of conversations during a private counseling session, or a group, joint or family counseling session that are separate from the rest of the individual's medical record.

Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, treatment frequency and modality, clinical test results, and any summary of the following items: Diagnosis, functional status, treatment plans, symptoms, prognosis, and progress notes to date.

Procedures:

1. **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** shall inform the patient of this limitation on access if the request will not be fulfilled.
2. **Patient Authorization Required:** In most circumstances, the **Organization's** employees 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.
3. **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:
    a. To carry out the following treatment, payment, or health care operations:
        i. Use by the originator of the psychotherapy notes for treatment;
        ii. 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
        iii. Use by the **Organization** to defend itself in a legal action or other proceeding brought by the patient.

b. To respond to the federal Department of Health and Human Services (HHS) to determine the **Organization's** compliance with HIPAA privacy rules;
c. To comply with the law;
d. To assist in health oversight activities regarding the originator of the psychotherapy notes;
e. To help coroners/medical examiners in the examination of deceased persons; and
f. To prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

In addition, psychotherapy notes may also be revealed, when necessary, to persons who are reasonably able to prevent or lessen a threat to the health or safety of a person, including the target of a threat in (f) above.

RELEVANT HIPAA REGULATIONS:

- §164.508(a) *Authorizations for uses and disclosures*

Continued on Next Page

Privacy 16.0 Uses and Disclosures for Which an Authorization is Required

FULL POLICY LANGUAGE:

Policy Purpose:

To inform **organization's** workforce of those situations when written patient authorization is required before **organization** may use or disclose PHI.

Policy Description:

Generally, under this policy, **organization** may not use or disclose PHI without a valid written authorization from the patient. When patient provides a valid authorization, the use and disclosure must be consistent with the authorization.

Procedures:

Psychotherapy Notes:

As noted in Privacy Policy 15, written authorization for the following uses or disclosures of psychotherapy notes, is not necessary when use or disclosure is necessary to:

a. To carry out the following treatment, payment, or health care operations:
    i. Use by the originator of the psychotherapy notes for treatment;
    ii. 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
    iii. Use by the **Organization** to defend itself in a legal action or other proceeding brought by the patient.
b. To respond to the federal Department of Health and Human Services (HHS) to determine the **Organization's** compliance with HIPAA privacy rules;
c. To comply with the law;
d. To assist in health oversight activities regarding the originator of the psychotherapy notes; and
e. To help coroners/medical examiners in the examination of deceased persons; and
f. To prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

In addition, psychotherapy notes may also be revealed, when necessary, to persons who are reasonably able to prevent or lessen a threat to the health or safety of a person, including the target of a threat in (f) above.

Marketing:

Organization must obtain an authorization for use or disclosure of PHI for marketing, except if the communication is in the form of a face-to-face communication made by **organization** to an individual, or a promotional gift of nominal value provided by the

organization. If the marketing involves financial remuneration to the **organization** from a third party, the authorization must state that such remuneration is involved.

Sale of Protected Health Information:
Organization must obtain an authorization for the disclosure of PHI which is a 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. When an authorization is given for sale of PHI, the authorization must state that the disclosure will result in remuneration being given.

Special Authorization Requirements for Marketing and Sale of PHI:

General Requirements:

1. An authorization is not valid, if the document submitted has any of the following defects:
    a. The expiration date has passed or the expiration event is known by the **Organization** to have occurred;
    b. The authorization has not been filled out completely, with respect to an element described by this policy, if applicable;
    c. The authorization is known by the **Organization** to have been revoked;
    d. The authorization violates this paragraph, or paragraphs below, if applicable; and
    e. Any material information in the authorization is known by the **Organization** to be false.
2. An authorization for use or disclosure of PHI may not be combined with any other document to create a compound authorization, except as follows:
    a. 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 research study, including another authorization for the use or disclosure of PHI for such research or a consent to participate in such research;
    b. 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
    c. 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 under this section, 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.
3. The **Organization** may not condition treatment, payment, or enrollment in a health plan, or eligibility for benefits on the provision of an authorization, except:
4. The **Organization** may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of PHI for such research under this policy;
    a. The **Organization** 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:

i. 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
ii. The authorization is not for a use or disclosure of psychotherapy notes.

5. The **Organization** may require an authorization for release to a third party before providing health care that is solely for the purpose of creating PHI for disclosure to a third party.
6. An individual may revoke an authorization provided under this policy at any time, provided that the revocation is in writing, except to the extent that:
    a. The **Organization** has taken action in reliance thereon; and
    b. 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.
7. The **Organization** must document and retain any signed authorization.

Core Elements and Requirements:

1. Core elements. A valid authorization under this section must contain at least the following elements (but may contain additional information):
    a. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
    b. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
    c. 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;
    d. 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;
    e. 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
    f. 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.
2. In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:
    a. The individual's right to revoke the authorization in writing, and either:
        i. The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or
        ii. To the extent that the information in paragraph (1) above is included in the notice of privacy practices.

b. The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:
    i. The **Organizatio**n may not condition treatment, payment, enrollment, or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in this policy applies; or
    ii. The **consequences** to the individual of a refusal to sign the authorization when, in accordance with this policy (i.e., for research, health plan eligibility, underwriting purposes, and risk rating determinations), the **Organization** can condition treatment, enrollment in a health plan, or eligibility for benefits on failure to obtain such authorization; and
    iii. 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.
3. The authorization must be written in plain language.
4. If the **Organization** seeks an authorization from an individual for a use or disclosure of PHI, the **Organization** must provide the individual with a copy of the signed authorization.

RELEVANT HIPAA REGULATIONS:

- §164.508 *Uses and Disclosures for Which an Authorization is Required*

Continued on Next Page

Privacy 17.0 Uses and Disclosures, No Authorization 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 obtain written patient authorization.

Policy Description:

Under several circumstances, the HIPAA Privacy Rule permits **organization** to use or disclose PHI without written patient authorization. Generally, these circumstances are circumstances under which the law requires such use or disclosure.

Procedures:

Uses and Disclosures Required by Law:

1. The **Organization** may 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. The **Organization** must disclose PHI as required by law 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.

Uses and Disclosures for Public Health Activities:

1. The **Organization** may disclose PHI related to public health activities if:
   a. A public health authority that is authorized by law to collect or receive such information, request the PHI 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
   b. It is necessary to report child abuse or neglect.
2. 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 individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or
d. To conduct post-marketing surveillance.

3. 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. An employer, about an individual who is a member of the workforce of the employer, if:
   a. The Covered Entity is the employee's health care provider and requests the information:
      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, or under State law having a similar purpose to record such illness or injury, or to carry out responsibilities for workplace medical surveillance; or
4. 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:
   a. By giving a copy of the notice to the individual at the time the health care is provided; or
   b. 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.
5. A school, about an individual who is a student or prospective student of 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 as an unemancipated minor.

If the covered entity described in (1) through (5) immediately above, is also a public health authority, the covered entity may use protected health information in all cases in which it is permitted to disclose such information for the pubic health activities specified in (1) through (5) above.

PHI may also be used or disclosed without authorization or affording an individual the opportunity to agree or object under the following circumstances.

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;
    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, 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 health care 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 "Uses and Disclosures for Health Oversight Activities," above, does not \t 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 covered entity may use PHI for health oversight activities as permitted by this policy.

Uses and Disclosures About Decedents:

1. Coroners and medical examiners: The **Organizatio**n 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 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. Board approval of a waiver of authorization is made available;
    b. 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:

1. 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;
2. 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
3. Does not have any member participating in a review of any project in which the member has a conflict of interest.

c. (Reviews preparatory to research). The **Organization** obtains from the researcher 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 researcher in the course of the review; and
   iii. The PHI for which use or access is sought is necessary for the research purposes.

d. (Research on decedent's information). The **Organization** obtains from the researcher:
   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 individuals; and
   iii. Representation that the PHI for which use or disclosure is sought is necessary for the research purposes.

e. 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 individuals based on, at least, the presence of the following elements:
         a. An adequate plan to protect the identifiers that lead to individual patients 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.

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

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

f. 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;

g. 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 individuals 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

iv. 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.

RELEVANT HIPAA REGULATIONS:

- §164.501 *Uses and Disclosures for Health Care Operations*
  §164.512 *Consent or Authorization Not Required*

Privacy 18.0 Uses and Disclosures Requiring Patient Opportunity to Agree or Object

FULL POLICY LANGUAGE:

Policy Purpose:

To inform employees of the situations under which a patient must be given an opportunity to agree or object to use or disclosure of their PHI.

Policy Description:

Under several circumstances, before **organization** may use or disclose an individual's PHI, that person must be given an opportunity to agree or object to the use or disclosure.

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 of this section.

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. The requirement of opportunity to agree or prohibit applies in the following circumstances:

Use and Disclosure for Facility Directories:

1. Permitted uses and disclosure. Except when an objection is expressed, the **Organization** may:
    a. Use the following PHI to maintain a directory of individuals in its facility:
        i. The individual's name;
        ii. The individual's location in the **Organization's** facility;
        iii. The individual's condition described in general terms that does not communicate specific medical information about the individual; and
        iv. The individual's religious affiliation; and
    b. Use or disclose for directory purposes such information:
        i. To members of the clergy; or
        ii. Except for religious affiliation, to other persons who ask for the individual by name.
2. Opportunity to object: The **Organization** must 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.
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 by this section for the facility's directory, if such disclosure is:
    i. Consistent with a prior expressed preference of the individual, if any, that is known to the **organization**; and
    ii. In the individual's best interest as determined by the **organization**, in the exercise of professional judgment.
b. The **Organization** must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes when it becomes practicable to do so.

Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes:

1. Permitted uses and disclosures.
    a. 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.
    b. 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.
2. Uses and disclosures with the individual present: If the individual is present for, or otherwise available prior to, a use or disclosure permitted by 45 CFR 164.510 and has the capacity to make health care decisions, the **Organization** may use or disclose the PHI if it:
    a. Obtains the individual's agreement;
    b. Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
    c. Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to the disclosure.
3. 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, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. The **Organization** may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.
4. 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

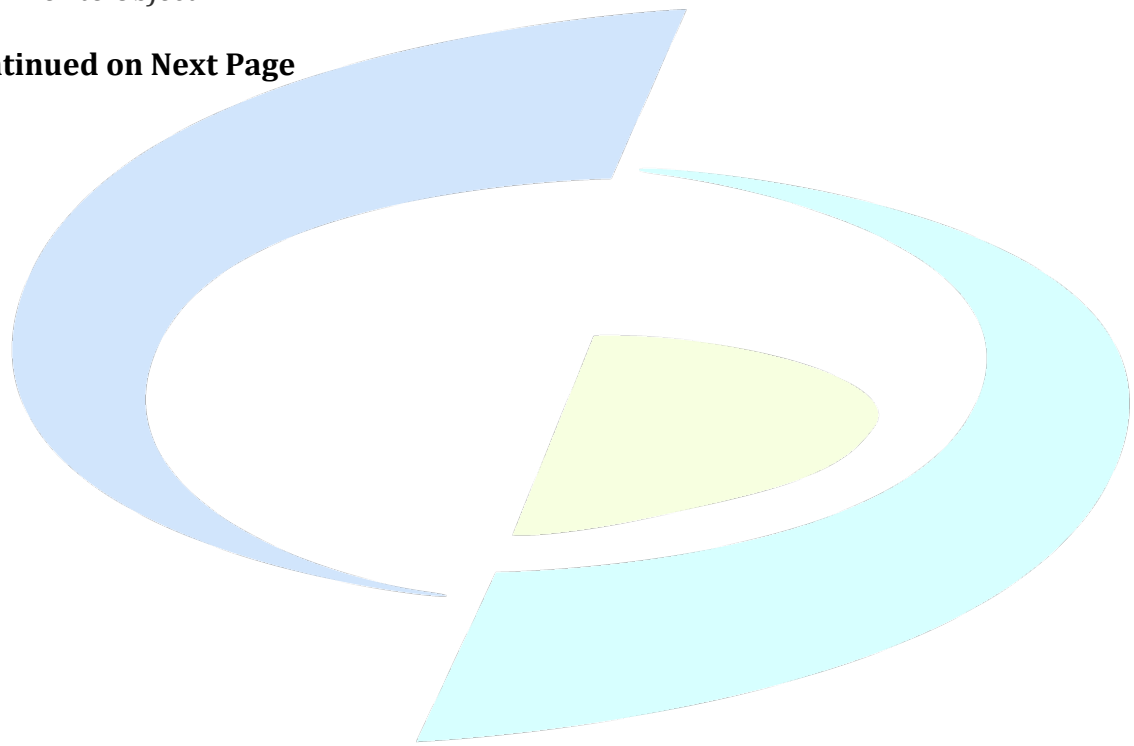
in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by this section.

5. 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**.

RELEVANT HIPAA REGULATIONS:

- §164.510 *Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object*

Continued on Next Page



Privacy 19.0 Uses and Disclosures of Workers Compensation Information

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:

An employee filing a claim for Workers Compensation due to an on-the-job injury consents to certain conditions. One of those conditions is, at the employer's request, they will submit to an examination by **organization** to determine the validity of their claim. This information is then available, with certain restrictions, to the employee, employer, state workers compensation board, or representative of any of these to assist in resolving the claim.

Employees filing a Workers Compensation claim waive all provider-patient privilege of information or results regarding any condition or complaint **reasonably related to the condition that they are claiming compensation for.**

Procedures:

1. After receipt of written request to the employee, employer, state board of workers compensation, or workers compensation insurance carrier for the employer, **Organization** shall release, within a reasonable amount of time, copies of medical records or verbal communications, that reasonably relate to the work injury.
2. Requests for copies of medical records, which extend beyond the scope of the work-related injury, need to be accompanied by a written authorization from the patient/employee.
3. **Organization** shall furnish legible duplicates of written material requested by employees, employers, insurance carriers, and state boards of workers compensation. Certified copies shall be furnished upon request.

RELEVANT HIPAA REGULATIONS:

- §164.512 *Consent or Authorization Not Required*

Privacy 20.0 Breach Notification

FULL POLICY LANGUAGE:

Policy Purpose:

To provide guidance for breach notification by **organization** when impermissible or unauthorized access, acquisition, use and/or disclosure of **Organization's** PHI occurs.

Policy Description:

This policy describes **organization's** legal responsibilities in the event of a PHI breach.

Procedures:

Determination of Breach:

An "acquisition, access, use, or disclosure in a manner not permitted is **presumed to be a breach** unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment" of at least the following factors:

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

The following are NOT considered to be breaches:

1. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or 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 the Privacy Rule;
2. Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI 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 the Privacy Rule; and
3. A disclosure of PHI 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.

Discovery of Breach:

A breach of PHI shall be treated as "discovered" as of the first day on which an incident that may have resulted in a breach is known to the **Organization**, or, by exercising reasonable

diligence would have been known to the **Organization** (includes breaches 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 agent (i.e. a business associate acting as an agent of the organization) of the **Organization.**

Following the discovery of a potential breach, the **Organization** shall begin an investigation, conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed to have been accessed, acquired, used, or disclosed as a result of the breach. The **Organization** shall also begin the process of determining 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.).

Procedures for Investigation:

1. **Naming of the Investigator:**
   The **Organization** shall name an individual to act as the investigator of the breach (i.e., privacy officer, security officer, risk manager, etc.). The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others as appropriate (i.e., administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.) The investigator shall be the key facilitator for all breach notification processes to the appropriate entities (i.e., HHS, media, law enforcement officials, etc.). All documentation related to the breach investigation, including the risk assessment and notifications made, shall be retained for a minimum of six (6) years.
2. **Risk Assessment:**
   For an acquisition, access, use, or disclosure of PHI to constitute a breach, it must otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach.

   An "acquisition, access, use, or disclosure in a manner not permitted is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment" of at least the following factors:
   - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
   - The unauthorized person who used the PHI or to whom the disclosure was made;
   - Whether the PHI was actually acquired or viewed; and
   - The extent to which the risk to the PHI has been mitigated.

The **Organization** shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. The **Organization** has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, the **Organization** will then determine the need to move forward with breach notification. The **Organization** may make breach notifications without completing a risk assessment.

3. **Breach Notification:**
   a. **Timeliness of Notification:** Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. It is the responsibility of the **Organization** to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.
   b. **Delay of Notification Authorized for Law Enforcement Purposes:** If a law enforcement official states to the **Organization** that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the **Organization** shall:
      i. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the time period specified by the official; or
      ii. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.
4. **Content of the Notification:**
   The notice shall be written in plain language and must contain the following information:

   a. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
   b. 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);
   c. Any steps the individual should take to protect themselves from potential harm resulting from the breach;
   d. A brief description of what the **Organization** is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and
   e. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.
5. **Methods of Notification:**
   The method of notification will depend on the individuals/entities to be notified.

The following methods must be utilized accordingly:

a. **Notice to Individual(s):** Notice shall be provided promptly and in the following form:
    i. Written notification by first-class mail to the individual at their last known address or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If the **Organization** knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or personal representative shall be carried out. Examples:
        a. The **Organization** may send one breach notice addressed to both a plan participant and the participant's spouse or other dependents under the plan who are affected by a breach, if they all reside at a single address and all individuals to which the notice applies are clearly identified on the notice. When a plan participant (and/or spouse) is not the personal representative of a dependent under the plan, however, address a breach notice to the dependent himself or herself; and
        b. In the limited circumstance that an individual affirmatively chooses not to receive communications from a health care provider at any written addresses or email addresses *and* has agreed only to receive communications orally or by telephone, the provider may telephone the individual to request and have the individual pick up their written breach notice from the provider directly. In cases in which the individual does not agree or wish to travel to the provider to pick up the written breach notice, the health care provider should provide all of the information in the breach notice over the phone to the individual, document that it has done so, and the Department will exercise enforcement discretion in such cases with respect to the ''written notice'' requirement.
b. **Substitute Notice:** In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in cases where there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.
    i. In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.

ii. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the **organization's** website, or a conspicuous notice in a major print or broadcast media in **Organization's** geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active or at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

iii. If the **Organization** determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

6. **Notice to Media:**
Notice shall be provided to prominent media outlets serving the state and regional area (of the breached patients) when the breach of unsecured PHI affects 500 or more of the **Organization's** patients of a State or jurisdiction.
   a. The Notice shall be provided in the form of a press release.
   b. What constitutes a prominent media outlet differs depending upon the state or jurisdiction where the **Organization's** affected patients reside. For a breach affecting more than 500 individuals across a particular state, a prominent media outlet may be a major, general interest newspaper with a daily circulation throughout the entire state. In contrast, a newspaper serving only one town and distributed on a monthly basis, or a daily newspaper of specialized interest (such as sports or politics) would not be viewed as a prominent media outlet. Where a breach affects more than 500 individuals in a limited jurisdiction, such as a city, then a prominent media outlet may be a major, general-interest newspaper with daily circulation throughout the city, even though the newspaper does not serve the whole State.
7. **Notice to Secretary of HHS:**
Notice shall be provided to the Secretary of HHS as follows below. The Secretary shall make available to the public on the HHS Internet website a list identifying covered entities involved in all breaches in which the unsecured PHI of more than 500 patients is accessed, acquired, used, or disclosed.
   a. For breaches involving 500 or more individuals, the **organizatio**n shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.
   b. For breaches involving fewer than 500 individuals, the **organization** will maintain a log of the breaches. The breaches may be reported during the calendar year or no later than 60 days after the end of that calendar year in which the breaches were discovered (Instructions for submitting the logged breaches are provided at www.hhs.gov).

8. **Maintenance of Breach Information/Log:**
   As described above and in addition to the reports created for each incident, the **Organization** shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected. The following information should be collected/logged for each breach (see sample Breach Notification Log):
   a. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known;
   b. A description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.);
   c. A description of the action taken with regard to notification of patients, the media, and the Secretary regarding the breach;
   d. The results of the risk assessment; and
   e. Resolution steps taken to mitigate the breach and prevent future occurrences.
9. **Business Associate Responsibilities:**
   Business Associates are directly liable for impermissible uses and disclosures, provision of breach notification to the covered entity, completing breach risk assessments, breach documentation requirements, and civil and criminal penalties for violations.

   The Business Associate of the **Organization** that accesses, creates, maintains, retains, modifies, records, stores, transmits, destroys, or otherwise holds, uses, or discloses Unsecured PHI shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify the **Organization** of such breach.

   Such notice shall include the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during such breach. The Business Associate shall provide the **Organization** with any other available information that the organization is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the Business Associate of discovery of a breach, the **Organization** will be responsible for notifying affected individuals, unless otherwise agreed upon by the Business Associate to notify the affected individuals (note: It is the responsibility of the **organization** to document this notification).
10. **Workforce Training:**
    The **Organization** shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and promptly report breaches within the **Organization**, as well as return or destroy PHI, as appropriate for the incident. Workforce members that

assist in investigating, documenting, and resolving breaches are trained on how to complete these activities.

a. **Complaints:** The **Organization** must provide a process for individuals to make complaints concerning the **organization's** patient privacy policies and procedures or its compliance with such policies and procedures. Individuals have the right to complain about the **Organization's** breach notification processes.
b. **Sanctions:** The **Organization** shall have in place and apply appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures.
c. **Retaliation/Waiver:** The **Organization** may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. The **Organization** may not require individuals to waive their privacy rights under as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

RELEVANT HIPAA REGULATIONS:

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

Continued on Next Page

Privacy 21.0 Notice of Privacy Practices

FULL POLICY LANGUAGE:

Policy Purpose:

Patients are entitled to an explanation of their rights with respect to uses and discloses of their PHI. The Privacy Rule requires organization to describe its privacy practices in plain English, in a document called a Notice of Privacy Practices. **Organization** must give patients a copy of this document.

Policy Description:

Organization must make its Notice of Privacy Practices ("Notice") available to all patients, 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.

Procedures:

Notice Content Requirements:

The Notice shall contain the following content:

1. **Header:** The header contains a brief summary stating how notice describes how medical information about patients may be used and disclosed and how patients can get access to this information.
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. The description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by state and federal law;
    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. A statement that other uses and disclosures will be made only with the individual's written authorization, and that the individual may revoke this authorization at any time in writing; and
    d. A statement that **organization** may contact individuals for: (i) Appointment reminders or to provide information regarding treatment alternatives or other health-related benefits, including services that may be of interest to the individual; or (ii) fundraising.
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. Inspect and copy his or her PHI;
b. Amend his or her PHI;
c. Receive an accounting of disclosures of his or her PHI;
d. Request restrictions on certain uses and disclosures of information (the notice must contain a statement that the **organization** is not required to agree to the requested restriction);
e. Receive confidential communications of PHI; and
f. Obtain a paper copy of the Notice of Privacy Practices upon request.

4. **Provider Duties:** The Notice must indicate the following:
   a. **Organization's** providers must maintain the privacy of PHI and provide individuals with notice of **organization's** legal duties and privacy practices;
   b. **Organization** must abide by the terms of the Notice currently in effect; and
   c. 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 individuals with a revised Notice.
5. **Complaints:** The Notice must explain that individuals 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.

Notice Dissemination and Publication Requirements:

1. The **Organization** must provide the Notice to its patients 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 individuals to take with them. (When the patient 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 patients 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.

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.

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 obtain acknowledgement of the Notice during the intake process.

Revisions to the Notice of Privacy Practices:

1. The **Organization** must promptly revise 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 in service delivery areas.
4. **Organization** must post the revised notice on its website.

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.

RELEVANT HIPAA REGULATIONS:

- §164.520(b) *Content of Notice of Privacy Practices*
- §164.520(c)(2) *Provision of Notice of Privacy Practices*

Privacy 22.0 Social Media

FULL POLICY LANGUAGE:

Policy Purpose:
To provide rules for acceptable social media use.

Policy Description:
This policy outlines the safeguards employees 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**.

Patient Privacy:

- Posting patient information, commentary, or photographs on professional or personal social media sites requires written authorization from the patient.
- Workforce members should contact their supervisors, or the Privacy Officer, to obtain a copy of the form.
- Once the form is obtained, a copy of the form is provided to the patient and the original authorization is placed in the patient's medical record.
- Members of the workforce may not tape-record or video-record in patient treatment areas, unless written permission is given by the Privacy Officer, the provider(s) and the patients involved.
- If any photos, tape-recordings, or video-recordings, contain images of other patients, written authorization from those patients must also be obtained.
- **Organization** staff and providers may not take personal photos, video, or audio recordings in patient care areas, so as to avoid inadvertently capturing patients or patient information.
- Photos, images, or a narrative a workforce member believes to be de-identified may in fact be recognizable by an individual patient. Therefore, permission should be obtained from the Privacy Officer prior to posting any photos, images, or narratives involving patients or patient information even if they are thought to be de-identified.
- Providers may video or audio record patients for treatment purposes, after receiving written patient authorization. Such recording may only be done using electronic devices that have been approved for such purpose by the Security Officer.
- Workforce members who suspect unauthorized disclosure of patient information via social media, or any suspected unauthorized photographing, filming, or recording, shall promptly report such suspicions to the Privacy Officer.

Interacting with Patients on Social Media:

- Workforce members may not connect with patients or their family members using social media.
- Workforce members should not accept “Friend” requests from patients on social media sites such as Facebook, nor should workforce members send such requests.

Continued on Next Page

Privacy 23.0 Complaints

FULL POLICY LANGUAGE:

Policy Purpose:

To maintain effective reporting for 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.

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. **Organization** strives to ensure that data breaches are responded to in an appropriate fashion, in accordance with the HIPAA Breach Notification Rule and other applicable law. Individuals have the right to make complaints concerning **Organization's** compliance with the HIPAA Privacy Rule and its HIPAA privacy policies and procedures ("Privacy Complaints"). Individuals also have the right to make complaints concerning the **Organization's** breach notification process and compliance with the Breach Notification Rule.

Procedures:

Processing a Complaint:

1. **Organization's** Notice of Privacy Practices must notify all patients (or their personal representatives) of their right to complain to **Organization** or the Department of Health and Human Services ("HHS").
2. Complaints may be made in person, or by telephone or mail.
3. Workforce members should forward complaints to the Privacy Officer.
4. Upon receipt of any complaint, 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 an investigation is warranted. If an investigation is warranted, the Privacy Officer shall conduct the investigation and determine if a violation of the HIPAA Privacy Rule, the HIPAA Breach Notification Rule, or **Organization's** HIPAA privacy or breach notification policies and procedures has occurred. The Privacy Officer should make all reasonable efforts to complete the investigation in a timely manner.
6. Upon completion of the investigation, 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 individual who made the complaint within 30 days from the Privacy Officer's receipt of the complaint.

7. 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 24.0).
8. 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(d) *Complaints*

Continued on Next Page

Privacy 24.0 Sanctions

FULL POLICY LANGUAGE:

Policy Purpose:

To ensure that appropriate sanctions will be applied to employees who violate the requirements of the HIPAA Privacy Rule and/or **Organization's** HIPAA privacy policies and procedures. To ensure that appropriate sanctions will be applied to employees who violate the requirements of the HIPAA Breach Notification Rule and/or **Organization's** HIPAA Breach Notification Rule policies and procedures.

Policy Description:

It is **Organization's** policy to impose sanctions, as applicable, for violations of **Organization's** policies and procedures regarding workforce HIPAA compliance. It is also **Organization's** policy to monitor compliance with HIPAA policies and to mitigate, to the extent practicable, any harm resulting from inappropriate use or disclosure of protected health information.

Procedures:

Sanctions:

1. When a concern arises regarding a potential violation of the HIPAA Privacy Rule or Breach Notification Rule, the Privacy Officer shall promptly investigate.
2. The Privacy Officer shall uniquely and consistently apply corrective disciplinary action when warranted.
3. The Privacy Officer may consider several criteria when determining the appropriate disciplinary measure.
    a. What was the intent behind the inappropriate use or disclosure of PHI?
        i. Was the use or disclosure unintentional?
        ii. Was the use or disclosure unintentional, and did the use or disclosure result in a reportable breach?
        iii. Was the use or disclosure intentional?
    b. What is the risk to the **Organization** resulting from the inappropriate use or disclosure?
        i. Is there a potential risk for patient harm?
        ii. Is there a risk of harm to the **Organization**?
        iii. Is there a risk the public may be affected by the inappropriate use or disclosure?
    c. What is the history of the employee or workforce member's work performance?
        i. Has the employee or workforce member previously been disciplined for previous inappropriate use or disclosure of PHI?
        ii. Has the employee or workforce member been subject to a series of progressive discipline actions, related or unrelated to privacy of PHI?

iii. What is the history of **Organization's** disciplinary actions for similar infractions (whether privacy-related or otherwise) committed by *other* employees or workforce members?

d. Are there mitigating circumstances that would support reducing the disciplinary/corrective action in the interest of fairness and consistency?

4. In **Organization's** discretion, inappropriate use and/or disclosures of PHI may be divided into the following three levels with recommended corresponding disciplinary action for each:
   a. **Level 1 Infraction:**
      i. **Nature of Infraction:** unintentional, resulting in no breach.
      ii. **Description of Infraction:** Infraction occurs when workforce member unintentionally or carelessly accesses, reviews, or reveals PHI to themselves or to others, either without a legitimate need to know, or beyond what the minimum necessary standard permits.
      iii. **Examples of Infraction Include:**
         1. Discussing PHI in public areas, such as elevators and lobbies.
         2. Inadvertently typing in the wrong patient's name and viewing the wrong patient's PHI as a result.
         3. Leaving PHI accessible in a work area, such as leaving patient medical records unattended in a meeting room.
      iv. **Recommended Discipline:** Recommended discipline can consist of a verbal warning, and/or additional HIPAA training.
   b. **Level 2 Infraction:**
      i. **Nature of Infraction:** an unintentional infraction that results in a reportable breach.
      ii. **Description of Infraction:** Infraction occurs when a workforce member unintentionally or carelessly accesses, reviews, or reveals PHI to themselves or others without a legitimate need to know or beyond what the minimum necessary standard requires, AND a reportable breach results.
      iii. **Examples of Infraction Include:**
         1. Faxing or mailing the wrong patient's information to another entity, resulting in a breach.
         2. Inappropriately accessing or disclosing a patient's medical information, either in disregard of minimum necessary standard, or when the workforce member's role does not authorize access to PHI.
         3. Compromising a password by sharing it, resulting in access to PHI.
      iv. **Recommended Discipline:** Recommended discipline varies depending on the circumstances. Recommended discipline can range from a written reprimand, final warning, suspension, or unpaid leave, up to, in the case of multiple severe infractions that lead to breaches, termination of employment.

c. **Level 3 Infraction:**
   i. **Nature of Infraction:** Intentional (deliberate and on purpose).
   ii. **Description of Infraction:** An intentional infraction occurs when a workforce member accesses, reviews, or discusses PHI either for personal financial or other gain, or with malicious intent (intent to harm the organization, a patient, or the public); a workforce member willfully, and with gross negligence, uses and/or discloses PHI, or destroys PHI; or a workforce member knowingly violates federal and/or state laws and regulations protecting PHI privacy and security.
   iii. **Examples of Infraction Include:**
      1. Deliberate inappropriate access of medical records of the workforce member's family, friends, acquaintances, or prominent individuals.
      2. Intentional unauthorized disclosure of patient information to a third party, including to a friend, relative, or the media.
   iv. **Recommended Discipline:** The recommended discipline varies depending on the circumstances. Recommended discipline ranges from a written reprimand, a final warning, a suspension, or unpaid leave, to termination.

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.

Mitigation:

1. In response to a report for information about a workforce member's or business associate's unauthorized use or disclosure of PHI, **Organization** shall act promptly to mitigate (reduce) any known or reasonably anticipated harmful effects from the disclosure.
2. **Organization** should promptly identify who made the unauthorized use or disclosure, and apply appropriate sanctions.
3. **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.
4. **Organization** shall take any and all other appropriate action to prevent further use or disclosure.
5. **Organization**, in accordance with the HIPAA Breach Notification Rule, shall notify the patient or patients whose PHI was or were the subject of the unauthorized use or disclosure.
6. **Organization**, in accordance with the HIPAA Breach Notification Rule, shall notify HHS, the media, and/or any other individuals or entities who must receive notification.
7. **Organization** shall document all mitigation efforts and retain such documentation for at least six (6) years.

RELEVANT HIPAA REGULATIONS:

- 45 CFR 164.530(e) *Sanctions*
- 45 CFR 164.530(f) *Mitigation*

Continued on Next Page

Privacy 25.0 No Retaliation; No Waiver of Rights

FULL POLICY LANGUAGE:

Policy Purpose:

To ensure individuals who file complaints are not intimidated or retaliated against by **Organization** or any workforce member. To ensure that individuals are not subjected to waiving their rights to complain under the HIPAA Privacy Rule and the HIPAA Breach Notification Rule in order to receive treatment.

Policy Description:

Organization may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right under the Privacy Rule, Breach Notification Rule, or **Organization's** policies and procedures pertaining to same. In addition, organization may not require individuals to waive their rights to complain under HIPAA, as a condition of the provision of treatment.

Procedures:

Refraining from Intimidating or Retaliatory Acts:

1. **Organization** shall prohibit the taking of any intimidating or retaliatory acts against any individual or other person (including a workforce member) for:
    a. Exercising their rights or participating in any process established by the HIPAA Rules, such as filing a complaint with HHS about **Organization's** privacy policies or practices; or breach notification process, policies, or practices;
    b. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing authorized by the HIPAA Rules; or
    c. Opposing any act or practice that violates the HIPAA Rules, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of HIPAA.
    d. Disclosing PHI, if:
        i. 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 individuals, workers, or the public; **and**
        ii. 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.**
    e. Disclosing PHI to a law enforcement official in compliance with this Manual and with the HIPAA regulations.
2. Prohibited actions include any acts by **organization**, its workforce members, or business associates, that threaten, intimidate, coerce, harass, discriminate against,

or, take any other retaliatory action against an individual, because that individual has engaged in an activity mentioned in 1(a) through 1(e) above.

3. Any workforce member who is aware of, or believes he or she is the victim of, intimidating or retaliatory acts committed by a workforce member or business associate should report his or her concerns to the Privacy Officer. Such reports, so long as they are made in good faith, are also protected from retaliation.
4. 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.

No Waiver of Rights:

1. **Organization** may not require an individual to waive any complaint rights they have under the HIPAA regulations, and **organization's** policies and procedures, as a condition of treatment.
2. An individual who believes that **organization** has insisted on or required such a waiver, shall notify the Privacy Officer.
3. The Privacy Officer shall review the allegations of the complaining individual.
4. Upon conclusion of investigation, the Privacy Officer shall impose appropriate sanctions.

RELEVANT HIPAA REGULATIONS:

- 45 CFR 164.530(g) *Refraining from intimidating or retaliatory acts*
- 45 CFR 164.530(h) *Waiver of Rights*

Continued on Next Page

Privacy 26.0 Uses and Disclosures for Treatment, Payment, and Health Care

FULL POLICY LANGUAGE:

Policy Purpose:

To set forth the conditions under which **organization** is not required to obtain written patient authorization before making a use or disclosure of PHI.

Policy Description:

Generally, to comply with the HIPAA Privacy Rule, **organization** must obtain a signed patient authorization before making a use or disclosure of protected health information. However, the HIPAA Privacy Rule does not require **organization** to obtain such authorization for treatment, payment or healthcare operations purposes. **Organization** will not seek to obtain written authorization for these purposes unless an exception requiring written authorization applies, or when state law requires such authorization.

Procedures:

Treatment:

1. "Treatment" is the provision, coordination, or management of health care and related services among health care providers **or by** a health care provider with a third party; consultation between health care providers regarding a patient; or the referral of a patient from one health care provider to another.
2. Generally, organization will not obtain written patient authorization prior to use or disclosure of PHI for treatment purposes.

Payment:

1. "Payment" encompasses the various activities of health care providers to obtain payment or be reimbursed for their services. Common payment activities of providers and health plans include, but are not limited to:
    a. Determining eligibility or coverage under a plan and adjudicating claims;
    b. Risk adjustments;
    c. Billing and collection activities;
    d. Reviewing health care services for medical necessity, coverage, justification of charges, and the like;
    e. Utilization review activities; and
    f. Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about the organization).
2. Generally, **organization** will not obtain written patient authorization prior to use or disclosure of PHI for payment purposes.

Healthcare Operations:

1. "Health care operations" are certain administrative, financial, legal, and quality improvement activities of an organization that are necessary to run its business and to support the core functions of treatment and payment. These activities include:
    a. Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;
    b. Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;
    c. Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims;
    d. Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;
    e. Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and
    f. Business management and general administrative activities, including those related to customer service, or sale or transfer of assets.
2. Generally, **organization** will not obtain written patient authorization prior to using or disclosing PHI for healthcare operations.

Exceptions Requiring Prior Written Authorization:
Generally, **organization** will not seek prior written authorization for treatment, payment, or healthcare operations purposes. However, **organization** will obtain such authorization if required by federal or state law. Federal law or state law may require obtaining written patient authorization before certain uses or disclosures of PHI can be made. These uses or disclosures for which authorization may be required include:

1. Disclosures that are required by state law, provided that **organization** discloses only the precise protected health information required, and only to the recipient required.
2. Disclosures to state, local, or federal governmental public health authorities to prevent or control disease, injury, or disability.
3. Disclosures to local, state, or federal governmental agencies to report suspected child abuse or neglect.
4. Disclosures to individuals or organizations under the jurisdiction of the federal Food and Drug Administration ("FDA"), such as drug or medical device manufacturers, regarding the quality or safety of drugs or medical devices.
5. Disclosures for health oversight audits, investigations, or disciplinary activities, provided that **organization** only disclose to a federal, state, or local governmental agency (or a private person or organization acting under contract with or grant of

authority from the governmental agency) that is authorized by law to conduct oversight activities.

6. Disclosures to police or other law enforcement officers regarding a crime that **organization** believed happened at its facility, provided that **organization** reasonably believes that the protected health information is evidence of a crime.
7. Disclosures to organizations involved in the procurement, banking, or transplantation of organs in order to facilitate organ donation and transplantation.

Minimum Necessary Standard:
Organization shall reasonably limit its disclosures of, and requests for, protected health information for payment and health care operations to the minimum necessary. **Organization** is not required to apply the minimum necessary standard to disclosures to or requests by a health care provider for treatment purposes.

RELEVANT HIPAA REGULATIONS:

- 45 CFR 164.506 *Treatment, Payment, or Healthcare Operations*

Continued on Next Page

Privacy 27.0 Sale of PHI

FULL POLICY LANGUAGE:

Policy Purpose:

To ensure sale of PHI is not conducted without prior written patient authorization.

Policy Description:

In accordance with the HIPAA Privacy Rule, **organization** shall not directly or indirectly receive remuneration, including non-financial benefits such as in-kind benefits, in exchange for any protected health information, unless prior written patient authorization is obtained.

Procedures:

1. If **organization** receives direct or indirect remuneration from or on behalf of a person or entity in exchange for PHI, that exchange is a sale of PHI. For such an exchange, a valid, written authorization must be obtained from the patient who is the subject of the information.
2. Prior to disclosing any PHI in exchange for direct or indirect remuneration, the Privacy Officer shall confirm whether the contemplated disclosure is a sale of PHI.
3. The disclosure of PHI for any of the following purposes is not considered a sale of PHI under the HIPAA Privacy Rule:
    a. Public health purposes;
    b. Research purposes, where the remuneration is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI;
    c. Treatment and payment purposes;
    d. The sale, transfer, merger, or consolidation of all or part of the **organization** with another organization, or an entity that will become another company following the transaction and due diligence related to this activity;
    e. To patients, where the patient requests access to PHI or an accounting of disclosures;
    f. Disclosures required by law; and
    g. Any other disclosures permitted by the HIPAA 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 or a fee otherwise expressly permitted by law.
4. Any disclosure of PHI in exchange for remuneration that meets an exception under HIPAA shall be further evaluated under applicable state law to ensure the exchange is permissible without written patient authorization under applicable state law.
5. If a disclosure of PHI meets the definition of a sale of PHI and an applicable exception does not apply, **organization** shall obtain prior written patient authorization.
    a. Patient authorization shall be obtained, and the authorization obtained shall meet the requirements of HIPAA and applicable state law. The authorization

shall specifically disclose that **organization** will receive direct or indirect remuneration in exchange for the PHI.

b. **Organization** shall place a copy of the signed authorization form in the patient's medical record.
c. Questions related to whether a transaction is a "Sale of PHI" disclosure that do not fall under an exception in (3) above, shall be reported to the Privacy Officer, who shall evaluate whether the disclosure constitutes a Sale of PHI.

6. Workforce members must:
    a. Ensure that any direct or indirect remuneration in exchange for PHI that constitutes a sale of PHI meets an exception and is permissible under HIPAA and applicable state law without individual authorization.
    b. For such activities that do not meet an exception, obtain patient authorization in the form and manner required by HIPAA and applicable state law, before a disclosure of PHI in exchange for remuneration.

RELEVANT HIPAA REGULATIONS:

- 45 CFR 164.508(a)(4) *Sale of PHI*

Continued on Next Page

Privacy 28.0 Policy for Disclosures by Whistleblowers and Workforce Member Crime Victims

FULL POLICY LANGUAGE:

Policy Purpose:

To outline the policies and procedures for disclosure of PHI by whistleblowers and workforce member crime victims.

Policy Description:

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.

In addition, under the "workforce member crime victims" exception to the Privacy Rule, workforce members who are victims of a crime may disclose protected health information about the suspected perpetrator of the criminal act; to law enforcement, provided the information disclosed is limited as described in this policy.

Procedures:

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:
    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.

5. To qualify as protected whistleblowing activity, the PHI disclosures listed above must be made to:
    a. An appropriate healthcare accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the **organization**; **or**
    b. 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**
    c. 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.
6. **Limitation on Disclosures:** Disclosures can only be made if the employee 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.

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.

RELEVANT HIPAA REGULATIONS:

- 45 CFR 164.502(j) *Disclosures by Whistleblowers and Workforce Member Crime Victims*

Privacy 29.0 Use or Disclosure for Specialized Government Functions

FULL POLICY LANGUAGE:

Policy Purpose:

To describe the circumstances under which PHI may be disclosed to government personnel and agencies for purposes of specialized government functions.

Policy Description:

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

This policy describes how organization will use and disclose PHI for these specialized government functions.

Procedures:

1. **Military and Veterans Activities.**
   a. **Armed Forces Personnel: Organization** may disclose to military authorities the PHI of individuals 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.
   b. 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.
   c. **Foreign Military Personnel: Organization** may use or disclose to the appropriate military authority the PHI of individuals who are foreign military personnel for the same purposes for which **organization** may use or disclose PHI regarding Armed Forces Personnel as described above.
2. **National Security and Intelligence Activities: Organization** may disclose PHI to authorized federal officials as necessary to conduct lawful intelligence, counter-intelligence, 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).
3. **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).

4. **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:
   a. The provision of healthcare to the individual;
   b. The health and safety of such individual or another inmate;
   c. The health and safety of the officers or employees, of or others at the correctional institution;
   d. 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;
   e. The administration and maintenance of safety, security, and good order of the correctional institution;
   f. 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.
5. **Minimum Necessary and Accounting for Disclosures:**
   a. **Minimum Necessary Rule:** If **organization** is permitted to make a disclosure of PHI as described above, **organization** may disclose only the information specified for the particular situation. If no specific information is specified for a particular situation, then **organization** may disclose only the minimum necessary PHI to accomplish the purpose of the disclosure.
   b. **Accounting for Disclosures: Organization** must keep a record of any disclosures made to law enforcement pursuant to this policy. This information shall be available to any individual who is the subject of such a disclosure and who requests an accounting of such a disclosure. Records regarding disclosures to law enforcement must be kept for at least 6 years after the date of the disclosure.

RELEVANT HIPAA REGULATION:

- 45 CFR 164.512(k) *Uses and Disclosures for Specialized Government Functions*

Privacy 30.0 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:

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** 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 create the limited data set.

Data Use Agreement:

1. **Organization** may use or disclose a limited data set, only if **organization** first obtains a signed, written obtains a Data Use Agreement (DUA) from the person/entity to whom the Limited Data Set is to be disclosed.
2. A DUA must be entered into before there is any use or disclosure of a limited data set to an outside party. A Data Use Agreement must:
    a. Establish the permitted uses and disclosures of such information by the limited data set recipient. The Data Use Agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate 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 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 Data Use Agreement;
        iii. Report to the **organization** any use or disclosure of the information not provided for by its Data Use Agreement of which it becomes aware;
        iv. Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
        v. Not identify the information or contact the individuals.
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 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*

Continued on Next Page

Glossary

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

Accounting of Disclosures of PHI: Information that describes a covered entity's disclosures of PHI other than for treatment, payment, and health care operations; disclosures made with written patient authorization; and certain other limited disclosures.

Administrative Tribunal: A judge or group of judges 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 agents. 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 Means: 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 addition of PHI to existing PHI contained in a designated record set.

Authorization: A patient's written statement of agreement to the use or disclosure of protected health information.

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) performs any function or activity involving the use or disclosure of PHI, **or** who provides services to **organization** that involve the disclosure of PHI. Such services include legal, accounting, consulting, data aggregation, management, and accreditation services.

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 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 may include patient medical and billing records; the enrollment, payment, claims, adjudication, and cases or medical management record systems maintained by or for a health plan; or information used in whole or in part to make care-related decisions.

Disclosure: To release, transfer, prove access to, or divulge PHI to a third party.

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic 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 in an effort to raise monies.

Health Care Operations: Quality assessment and improvement activities; reviewing the competence, qualifications, performance of health care professionals, conducting training programs, accreditation, certification, licensing, credentialing, underwriting, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits; conducting or arranging for medical review, legal services, and audition functions; business planning and development; business management (§164.501).

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, 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 individuals the right to access their protected information; the right to request that this information be amended; 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 individuals. 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 patient and his/her Personal Representative.

Individually Identifiable Health Information: Any information, including demographic information, collected from an individual 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; and
    a. Identifies the individual; or
    b. With respect to which there is a reasonable basis to believe that the information can 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.

Marketing: The provision of information about a product or service that encourages recipients of the communication to purchase or use the product or service.

Medical Record: A collection of documents, notes, forms, and test results that collectively document healthcare services provided to a patient in any aspect of health care delivery by a provider.

Minimum Necessary: The least amount of protected health information (PHI) needed to achieve the intended purpose of the use or disclosure of that PHI

Notice of Privacy Practices: A document required by the HIPAA Privacy Rule. The Notice of Privacy Practices must provide patients with information on how organization generally uses their PHI, and what patients' rights are with respect to that PHI.

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

Opt-Out: To make a choice to be excluded from services, procedures, or practices.

Payment. Activities undertaken by the Organization to obtain or provide reimbursement for the provision of health care. Activities for payment include eligibility of coverage determination, billing, claims management, collection activities, 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 a patient in making decisions related to health care Personal Representatives may have access to and/or request amendment of PHI relevant to their representative capacity, unless there is a reasonable belief that the patient has been or may be subjected to domestic violence, abuse, or neglect by such person, the release could endanger the patient, or in the exercise of professional judgment it is decided that it is not in the best interest of the patient to treat the person as the patient's personal representative.

Privacy Breach: A violation of the responsibility to follow privacy policy and procedure that results in the accessing of PHI by unauthorized personnel.

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): Individually identifiable health information that is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual;
- The provision of health care to an individual; or
- The past, present, or future payment for the provision of health care to an individual.

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

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.

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.

Use: To share, examine, or analyze protected health information.

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

Workforce: Employees, volunteers, trainees, 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 individuals are paid by the **Organization**.