HCBS Provider
8334986001
1467 Hark A Way Rd
Chester Springs, PA 19425
Generated Date: 12/7/2021

Privacy Rights & Operations Guide

HIPAA Privacy Rights and Operations Guide
HIPAA Security Summary

For the Practice of:
Home Community Based Services Provider, Inc
Publish Date: 11/28/2021

This guide has been created to serve Home Community Based Services Provider, Inc. It is intended to provide this organization and its workforce members with an overview of our daily operating policies and procedures and this organization's obligations relating to security and privacy standards for the use and disclosure of "protected health information" (PHI) under HIPAA, the Health Insurance Portability and Accountability Act of 1996.

This guide presents a simplified version of the fully detailed policies and procedures utilized to operate this Organization while maintaining the privacy and security of PHI. It should be used by workforce members and management as a quick reference to answer common questions about compliance operations and how to handle workplace situations so that HIPAA regulations are met and Patient Rights are upheld.

This document *is not* typically intended for outside distribution except as part of a wider investigation by regulators or other appropriate parties.

It is the responsibility of this Organization to conduct regular reviews of this document to incorporate updates as regulations change and/or to add more definition to the actual operational procedures utilized by this organization.

If you have any questions—or if you need further guidance on HIPAA Privacy or Security requirements, please contact the Privacy Officer (PO) or Security Officer (SO):

Privacy Officer
Home Community Services Based Provider, Inc.
1467 Harkaway Rd.
Chester Springs, PA 19425
610-453-5005
info@hcbsprovider.com

Security Officer
Home Community Services Based Provider, Inc.
1467 Harkaway Rd.
Chester Springs, PA 19425
610-453-5005
info@hcbsprovider.com

Section A: Privacy

Privacy, according to the HIPAA Privacy Rule, is an individual's right to control access and disclosure of their protected, "individually identifiable" health information. Besides giving individuals significant rights to understand and control how their health information is used, the Privacy Rule describes requirements for the use and disclosure of individuals' health information—protected health information (PHI)—by Covered Entity (CE) organizations subject to the Privacy Rule. PHI is considered "identifiable" if it contains any one or more of the 18 specific identifiers. (NOTE: See policy '*8s - Minimum Necessary'* for a complete list of the 18 identifiers)

1. Notice of Privacy Practices

Individuals have a right to receive a notice of the CE's privacy practices. The notice must be written in plain language and describe the ways in which the CE may use or disclose PHI. It also explains individual rights with respect to their health information, including the right to complain to Health and Human Services (HHS) and to the CE if they believe their privacy rights have been violated

Enter Any Notice of Privacy Practices: Home Community Based Services Provider, Inc.
NOTICE OF PRIVACY PRACTICES
(includes Omnibus changes as of March 2013)
Effective Date: 11/28/2021

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.
PLEASE REVIEW IT CAREFULLY.

If you have any questions about this Notice of Privacy Practices ('Notice'), please contact:

Privacy Officer: Cathy Stein, CEO

Phone Number: 610-453-5005

Section A: Who Will Follow This Notice?

This Notice describes Home Community Based Services Provider, Inc. (hereafter referred to as 'Provider') Privacy Practices and that of a ny workforce member authorized to create medical information referred to as Protected Health Information (PHI) which may be used for purposes such as Treatment, Payment and Healthcare Operations. These workforce members may include:

- all departments and units of the Provider.

- any member of a volunteer group.

- all employees, staff and other Provider personnel.

- any entity providing services under the Provider's direction and control will follow the terms of this notice. In addition, these entities, sites and locations may share medical information with each other for Treatment, Payment or Healthcare Operational purposes described in this Notice.

Section B: Our Pledge Regarding Medical Information

We understand that medical information about you and your health is personal. We are committed to protecting medical information about you. We create a record of the care and services you receive at the Provider. We need this record to provide you with quality care and to comply with certain legal requirements. This Notice applies to all of the records of your care generated or maintained by the Provider, whether made by Provider personnel or your personal doctor.

This Notice will tell you about the ways in which we may use and disclose medical information about you. We also describe your rights and certain obligations we have regarding the use and disclosure of medical information.

We are required by law to:

- Make sure that medical information that identifies you is kept private;

- Give you this Notice of our legal duties and privacy practices with respect to medical information about you; and

- Follow the terms of the Notice that is currently in effect.

Section C: How We May Use and Disclose Medical Information about You

The following categories describe different ways that we use and disclose medical information. For each category of uses or disclosures we will explain what we mean and try to give some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

- Treatment. We may use medical information about you to provide you with medical treatment or services. We may disclose medical information about you to doctors, nurses, technicians, health care students, or other Provider personnel who are involved in taking care of you at the Provider. For example, a doctor treating you for a broken leg may need to know if you have diabetes because diabetes may slow the healing process. In addition, the doctor may need to tell the dietitian if you have diabetes so that we can arrange for appropriate meals. Different departments of the Provider also may share medical information about you in order to coordinate different items, such as prescriptions, lab work and x-rays. We also may disclose medical information about you to people outside the Provider who may be involved in your medical care after you leave the Provider.

- Payment. We may use and disclose medical information about you so that the treatment and services you receive at the Provider may be billed and payment may be collected from you, an insurance company or a third party. For example, we may need to give your health plan information about surgery you received at the Provider so your health plan will pay us or reimburse you for the procedure. We may also tell your health plan about a prescribed treatment to obtain prior approval or to determine whether your plan will cover the treatment.

- Healthcare Operations. We may use and disclose medical information about you for Provider operations. These uses and disclosures are necessary to run the Provider and make sure that all of our

patients receive quality care. For example, we may use medical information to review our treatment and services and to evaluate the performance of our staff in caring for you. We may also combine medical information about many Provider patients to decide what additional services the Provider should offer, what services are not needed, and whether certain new treatments are effective. We may also disclose information to doctors, nurses, technicians, health care students, and other Provider personnel for review and learning purposes. We may also combine the medical information we have with medical information from other Providers to compare how we are doing and see where we can make improvements in the care and services we offer. We may remove information that identifies you from this set of medical information so others may use it to study health care and health care delivery without learning a patient's identity.

- Appointment Reminders. We may use and disclose medical information to contact you as a reminder that you have an appointment for treatment or medical care at the Provider.

- Treatment Alternatives. We may use and disclose medical information to tell you about or recommend possible treatment options or alternatives that may be of interest to you.

- Health-Related Benefits and Services. We may use and disclose medical information to tell you about health-related benefits or services that may be of interest to you.

- Fundraising Activities. We may use information about you to contact you in an effort to raise money for the Provider and its operations. We may disclose information to a foundation related to the Provider so that the foundation may contact you about raising money for the Provider. We only would release contact information, such as your name, address and phone number and the dates you received treatment or services at the Provider. If you do not want the Provider to contact you for fundraising efforts, you must notify us in writing and you will be given the opportunity to 'Opt-out' of these communications.

- Authorizations Required
We will not use your protected health information for any purposes not specifically allowed by Federal or State laws or regulations without your written authorization; this includes uses of your PHI for marketing or sales activities.

- Emergencies. We may use or disclose your medical information if you need emergency treatment or if we are required by law to treat you but are unable to obtain your consent. If this happens, we will try to obtain your consent as soon as we reasonably can after we treat you.

- Psychotherapy Notes
Psychotherapy notes are accorded strict protections under several laws and regulations. Therefore, we will disclosure psychotherapy notes only upon your written authorization with limited exceptions.

- Communication Barriers. We may use and disclose your health information if we are unable to obtain your consent because of substantial communication barriers, and we believe you would want us to treat you if we could communicate with you.

- Provider Directory. We may include certain limited information about you in the Provider directory while you are a patient at the Provider. This information may include your name, location in the Provider, your general condition (e.g., fair, stable, etc.) and your religious affiliation. The directory information, except for your religious affiliation, may also be released to people who ask for you by name. Your religious affiliation may be given to a member of the clergy, such as a priest or rabbi, even if they do not ask for you by name. This is so your family, friends and clergy can visit you in the Provider and generally know how you are doing.

- Individuals Involved in Your Care or Payment for Your Care. We may release medical information about you to a friend or family member who is involved in your medical care and we may also give information to someone who helps pay for your care, unless you object in writing and ask us not to provide this information to specific individuals. In addition, we may disclose medical information about you to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status and location.

- Research. Under certain circumstances, we may use and disclose medical information about you for research purposes. For example, a research project may involve comparing the health and recovery of all patients who received one medication to those who received another, for the same condition. All research projects, however, are subject to a special approval process. This process evaluates a proposed research project and its use of medical information, trying to balance the research needs with patients' need for privacy of their medical information. Before we use or disclose medical information for research, the project will have been approved through this research approval process, but we may, however, disclose medical information about you to people preparing to conduct a research project, for example, to help them look for patients with specific medical needs, so long as the medical information they review does not leave the Provider. We will almost always generally ask for your specific permission if the researcher will have access to your name, address or other information that reveals who you are, or will be involved in your care at the Provider.

- As Required By Law. We will disclose medical information about you when required to do so by federal, state or local law.

- To Avert a Serious Threat to Health or Safety. We may use and disclose medical information about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat.

- Email Use.
Email will only be used following this Organization’s current policies and practices and with your permission. The use of secured, encrypted e-mail is encouraged.

Section D: Special Situations

- Organ and Tissue Donation. If you are an organ donor, we may release medical information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

- Military and Veterans. If you are a member of the armed forces, we may release medical information about you as required by military command authorities. We may also release medical information about foreign military personnel to the appropriate foreign military authority.

- Workers' Compensation. We may release medical information about you for workers' compensation or similar programs.

- Public Health Risks. We may disclose medical information about you for public health activities. These activities generally include the following:

o to prevent or control disease, injury or disability;

o to report births and deaths;

o to report child abuse or neglect;

o to report reactions to medications or problems with products;

o to notify people of recalls of products they may be using;

o to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition; and

o to notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.

- Health Oversight Activities. We may disclose medical information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

- Lawsuits and Disputes. If you are involved in a lawsuit or a dispute, we may disclose medical information about you in response to a court or administrative order. We may also disclose medical information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

- Law Enforcement. We may release medical information if asked to do so by a law enforcement official:

o in response to a court order, subpoena, warrant, summons or similar process;

o to identify or locate a suspect, fugitive, material witness, or missing person;

o about the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement;

o about a death we believe may be the result of criminal conduct;

o about criminal conduct at the Provider; and

o in emergency circumstances, to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime.

- Coroners, Medical Examiners and Funeral Directors. We may release medical information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also release medical information about patients of the Provider to funeral directors as necessary to carry out their duties.

- National Security and Intelligence Activities. We may release medical information about you to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

- Protective Services for the President and Others. We may disclose medical information about you to authorized federal officials so they may provide protection to the President, other authorized persons or foreign heads of state or conduct special investigations.

- Inmates. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release medical information about you to the correctional institution or law enforcement official. This release would be necessary for the institution to provide you with health care, to protect your health and safety or the health and safety of others, or for the safety and security of the correctional institution.

Section E: Your Rights Regarding Medical Information about You

You have the following rights regarding medical information we maintain about you:

- Right to Access, Inspect and Copy. You have the right to access, inspect and copy the medical information that may be used to make decisions about your care, with a few exceptions. Usually, this includes medical and billing records, but may not include psychotherapy notes. If you request a copy of the information, we may charge a fee for the costs of copying, mailing or other supplies associated with your request.

- We may deny your request to inspect and copy medical information in certain very limited circumstances. If you are denied access to medical information, in some cases, you may request that the denial be reviewed. Another licensed health care professional chosen by the Provider will review your request and the denial. The person conducting the review will not be the person who denied your request. We will comply with the outcome of the review.

- Right to Amend. If you feel that medical information we have about you is incorrect or incomplete, you

may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for the Provider. In addition, you must provide a reason that supports your request.

- We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that:

o Was not created by us, unless the person or entity that created the information is no longer available to make the amendment;

o Is not part of the medical information kept by or for the Provider;

o Is not part of the information which you would be permitted to inspect and copy; or

o Is accurate and complete.

- Right to an Accounting of Disclosures. You have the right to request an 'Accounting of Disclosures'. This is a list of the disclosures we made of medical information about you. Your request must state a time period which may not be longer than six years and may not include dates before April 14, 2003. Your request should indicate in what form you want the accounting (for example, on paper or electronically, if available). The first accounting you request within a 12 month period will be complimentary. For additional lists, we may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

- Right to Request Restrictions. You have the right to request a restriction or limitation on the medical information we use or disclose about you for payment or healthcare operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that we not use or disclose information about a surgery you had. In your request, you must tell us what information you want to limit, whether you want to limit our use, disclosure or both, and to whom you want the limits to apply (for example, disclosures to your spouse). We are not required to agree to these types of request. We will not comply with any requests to restrict use or access of your medical information for treatment purposes.

You also have the right to restrict use and disclosure of your medical information about a service or item for which you have paid out of pocket, for payment (i.e. health plans) and operational (but not treatment) purposes, if you have completely paid your bill for this item or service. We will not accept your request for this type of restriction until you have completely paid your bill (zero balance) for this item or service. We are not required to notify other healthcare providers of these restrictions, that is your responsibility.

- Right to Receive Notice of a Breach. We are required to notify you by first class mail or by email (if you have indicated a preference to receive information by email), of any breaches of Unsecured Protected Health Information as soon as possible, but in any event, no later than 60 days following the discovery of the breach. "Unsecured Protected Health Information" is information that is not secured through the use of a technology or methodology identified by the Secretary of the U.S. Department of Health and Human Services to render the Protected Health Information unusable, unreadable, and undecipherable to unauthorized users. The notice is required to include the following information:

o a brief description of the breach, including the date of the breach and the date of its discovery, if known;

o a description of the type of Unsecured Protected Health Information involved in the breach;

o steps you should take to protect yourself from potential harm resulting from the breach;

o a brief description of actions we are taking to investigate the breach, mitigate losses, and protect against further breaches;

o contact information, including a toll-free telephone number, e-mail address, Web site or postal address to permit you to ask questions or obtain additional Information.

In the event the breach involves 10 or more patients whose contact information is out of date we will post a notice of the breach on the home page of our website or in a major print or broadcast media. If the breach involves more than 500 patients in the state or jurisdiction, we will send notices to prominent media outlets. If the breach involves more than 500 patients, we are required to immediately notify the Secretary. We also are required to submit an annual report to the Secretary of a breach that involved less than 500 patients during the year and will maintain a written log of breaches involving less than 500 patients.

- Right to Request Confidential Communications. You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or hard copy or e-mail. We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

- Right to a Paper Copy of This Notice. You have the right to a paper copy of this Notice. You may ask us to give you a copy of this Notice at any time. Even if you have agreed to receive this Notice electronically, you are still entitled to a paper copy of this Notice. You may obtain a copy of this Notice at our website. hcbsprovider.com

To exercise the above rights, please contact the individual listed at the top of this Notice to obtain a copy of the relevant form you will need to complete to make your request.

Section F: Changes to This Notice

We reserve the right to change this Notice. We reserve the right to make the revised or changed Notice effective for medical information we already have about you as well as any information we receive in the future. We will post a copy of the current Notice. The Notice will contain on the first page, in the top right hand corner, the effective date. In addition, each time you register at or are admitted to the Provider for treatment or health care services as an inpatient or outpatient, we will offer you a copy of the current Notice in effect.

Section G: Complaints

If you believe your privacy rights have been violated, you may file a complaint with the Provider or with the Secretary of the Department of Health and Human Services;

http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html

To file a complaint with the Provider, contact the individual listed on the first page of this Notice. All complaints must be submitted in writing. You will not be penalized for filing a complaint.

Section H: Other Uses of Medical Information

Other uses and disclosures of medical information not covered by this Notice or the laws that apply to us will be made only with your written permission. If you provide us permission to use or disclose medical information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose medical information about you for the reasons covered by your written authorization. You understand that we are unable to take back any disclosures we have already made with your permission, and that we are required to retain our records of the care that we provided to you.

Section I: Organized Healthcare Arrangement

The Provider, the independent contractor members of its Medical Staff (including your physician), and other healthcare providers affiliated with the Provider have agreed, as permitted by law, to share your health information among themselves for purposes of treatment, payment or health care operations. This enables us to better address your healthcare needs.

Our Organization creates record(s) of the care and services that patients receive from us. We need this record to provide them with quality care and to comply with certain legal requirements. Our NPP describes the ways in which we may use and disclose medical information about the patient. It also describes their rights and certain obligations we have regarding the use and disclosure of their medical information.

Our Organization always strives to follow all of the rules set down in our NPP. Any variation from our published practices that you notice should immediately be brought to the attention of the Organization's Security / Privacy Officer(s).

2. TPO (Treatment, Payment and Operations)

A CE may use or disclose PHI for its own treatment, payment or healthcare operations. Within our NPP, the following categories describe different ways that we may use and disclose patient PHI.

- **Treatment.** We may use medical information to provide a patient with medical treatment or services. We may disclose medical information about the patient to doctors, nurses, technicians, health care students, or other personnel who are involved in taking care of the patient within our Organization.

- **Payment.** We may use and disclose medical information about a patient so that the treatment and services received from the Organization may be appropriately billed and payment may be collected from the government, an insurance company or a third party.

- **Healthcare Operations.** We may use and disclose medical information about a patient for Organization operations. These uses and disclosures are necessary to run the Organization and make sure that all of our patients receive quality care.

3. Access, Use and Disclosure of PHI

General rules for access, use and disclosure of PHI are addressed within our NPP. *Minimum Necessary* principals are always applied to access, use, or in the disclosure of PHI, meaning only the least amount of information needed to perform the permitted task is utilized. (NOTE: See policy *'8s - Minimum Necessary'* for additional details)

- **Appointment Reminders.** We may use and disclose medical information to contact a patient as a reminder that they have an appointment for treatment or medical care at the Provider location.

- **Treatment Alternatives.** We may use and disclose medical information to tell a patient about or recommend possible treatment options or alternatives that may be of interest to them.

- **Health & Related Benefits and Services.** We may use and disclose medical information to tell a patient about health and related benefits or services that may be of interest to them.

- **Fundraising Activities.** none

- **Emergencies.** We may use or disclose a patient's medical information if they were to need emergency treatment or if we are required by law to treat them but are unable to obtain their consent. If this happens, we will try to obtain the patient's consent as soon as we reasonably can after treatment.

- **Communication Barriers.** We may use and disclose a patient's health information if we are unable to obtain their consent because of substantial communication barriers, and we believe they would want us to treat them if we could communicate with them.

- **Provider Directory.** Cathryn Stein, CEO & Compliance Officer, 610-453-5005, cathy@hcbsprovider.com

- **Individuals Involved in the Patient's Care or Payment for Care.** We may release medical information about a patient to a friend or family member who is involved in their medical care and to whom the patient has agreed it is permissible. We may also give information to someone who helps pay for their care. In addition, we may disclose medical information about a patient to an entity assisting in a disaster relief effort so that the family can be notified about their condition, status and location.

- **Research.** none

- **As Required By Law.** We will disclose medical information about a patient when required to do so by federal, state or local law.

- **To Avert a Serious Threat to Health or Safety.** We may use and disclose medical information about the patient when necessary to prevent a serious threat to their health and safety or the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat.

- **Organ and Tissue Donation.** If a patient is an organ donor, we may release medical information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

- **Military and Veterans.** If the patient is a member of the armed forces, we may release medical information about the patient as required by military command authorities.

- **Workers' Compensation.** We may release medical information about a patient for workers' compensation or similar programs.

- **Public Health Risks.** We may disclose medical information about a patient for public health activities. These activities generally include the following:
    - to prevent or control disease, injury or disability;
    - to report births and deaths;
    - to report child abuse or neglect;
    - to report reactions to medications or problems with products;
    - to notify people of recalls of products they may be using;
    - to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition; and
    - to notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if the patient agrees or when required or authorized by law.

- **Health Oversight Activities.** We may disclose medical information to a health oversight agency for activities authorized by law. For example, audits, investigations, inspections, and licensure.

- **Lawsuits and Disputes.** If a patient is involved in a lawsuit or a dispute, we may disclose medical information about them in response to a court or administrative order. We may also disclose medical information about them in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell that patient about the request or to obtain an order protecting the information requested.

- **Law Enforcement.** We may release medical information if asked to do so by a law enforcement official:
    - in response to a court order, subpoena, warrant, summons or similar process;
    - to identify or locate a suspect, fugitive, material witness, or missing person;
    - about the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement;
    - about a death we believe may be the result of criminal conduct;
    - about criminal conduct at the Provider; and
    - in emergency circumstances, to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime.

- **Coroners, Medical Examiners and Funeral Directors.** We may release medical information to a coroner or medical examiner. We may also release medical information about patients of the Practice to funeral directors as necessary to carry out their duties.

- **National Security and Intelligence Activities.** We may release medical information about a patient to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

- **Protective Services for the President and Others.** We may disclose medical information about a patient to authorized federal officials so they may provide protection to the President, other authorized persons or foreign heads of state or conduct special investigations.

- **Inmates.** If a patient is an inmate of a correctional institution or under the custody of a law enforcement official, we may release medical information about them to the correctional institution or law enforcement official.

4. Individual (Patient) Rights

The HIPAA Privacy Rule grants the following 'rights' regarding a patient's access to PHI and his/her right to control this information. A Covered Entity Organization typically 'owns' the records associated with the patient's PHI, but has certain responsibilities for its maintenance. Individuals have the right to inspect and obtain a copy of their PHI in a designated record set for as long as the CE maintains the information. Generally, the Privacy Rule requires CEs to retain certain documentation for at least six (6) years. Most healthcare organizations keep medical records for a much longer time frame, and individuals have the right to access their records for as long as the CE keeps them. Regardless of time, every patient has rights to facilitate the confidentiality, security, accuracy and integrity of his/her information.

- **Right to Access, Inspect and Copy Patient Information**

  - This patient 'Right' is often referred to as 'Release of Information'.

  - A patient has the right to access, inspect and copy medical information that is used to make decisions about his/her care. Usually, this includes medical and billing records, but does NOT include psychotherapy notes. (NOTE: Refer to our *'10s - Individual Access to PHI'* policy) for other important exceptions) If the patient requests a copy of the information, our Organization may charge a fee for the costs of processing, copying, mailing or other supplies associated with the request. If a patient provides us with permission to use or disclose medical information about them, they may revoke that permission, in writing, at any time. If they revoke their permission, we will no longer use or disclose medical information about them for the reasons covered by their written authorization. They will need to understand that we are unable to take back any disclosures we have already made with their permission, and that we are required to retain our records of the care that we provided to them by law.

  - We may deny a patient request to inspect and copy medical information in certain very limited circumstances. If they are denied access to medical information, in some cases, they may request that the denial be reviewed. Another licensed health care professional chosen by the Organization will review the request and the denial. The person conducting the review will not be the person who denied the request. Our Organization will comply with the outcome of the review and document all of the processes included with the review.

  Procedures for Inspection, Copying and Disclosure of PHI

  Include any company-specific procedures if applicable: none

  - ***If the patient asks us to speak to another physician (or provider of care),*** use Privacy / Security Combo form *'Js - Authorization to Disclose PHI'* to gain signed authorization and documentation that we have permission to provide patient identifiable information to another healthcare provider. Note: If information provided is to another provider of care and is to be used for 'treatment' (the provision of healthcare) there is ***not*** a strict requirement under

HIPAA to get an authorization signed; but it is a good practice that we try to follow, especially if the other provider is unknown to the organization/practice. Any release of information that requires an accounting of disclosures should be logged on Privacy / Security Combo form *'AAs - ROI Breach Patient's Rights Log'* even if the patient does not sign an authorization for that disclosure.

- ***If the patient asks us to disclose our written or copied patient information outside our organization***… the *'Js - Authorization to Disclose PHI'* is used to release information to a third party, which may or may not be another healthcare provider. If possible, get the patient to allow our practice to send the information directly to their provider of care, ensuring confidentiality and correct communications are observed. Depending on the purpose for the disclosure and type of third party (e.g., Adult Protective Services, Child Protective Services, Coroner/Medical Examiner, court order, employer, et al.), releasing the entire medical record and tracking for Accounting of Disclosures MAY or MAY NOT be required. none
  NOTE: The purpose behind a request for disclosure may also impact the fees we may charge for completing the request.

- ***If the patient asks us to request written or copied patient information from another provider of care outside our practice/organization*** …use *'Js - Authorization to Disclose PHI'* to authorize and request release of information. If written or copied patient information is to be used for 'treatment' (the provision of healthcare), there is not a strict requirement under HIPAA to get an authorization signed before we request the information; but it is a good practice that we try to follow, especially if the other provider is unknown to the organization/practice. Oftentimes, other providers of care will want the signed authorization, just for their own processing and protections.

- As regulatory standards and organizational policy dictate:
  - Record information disclosures in the *'AAs - ROI Breach Patient's Rights Log'.*
  - Be sure to calculate record copying fees according to State Statutes if the request is not going directly to another healthcare provider for treatment purposes. There are instances where charges are not appropriate, such as in payment and healthcare oversight processes. Refer to the organization's *Release of Information* policies for additional guidelines on relevant scenarios and the appropriate fees.
  - Be sure to validate and *if possible* get copies of the patient's or requestor's ID to store with the authorization. Some law enforcement agencies may not permit you to copy their ID or badges, and that is fine as long as you notate their ID number on the request, along with their affiliation, title, etc.
  - Refer to and use *'Js - Authorization to Disclose PHI'* as often as needed; be sure to get signed authorizations to go with subpoenas.
  - If a patient requests **electronic** copies of their medical records, we need to disclosure them in that format if they are kept electronically. Electronic copies are produced by Google Documents.

- All of the above documentation must be kept for the minimum 6 year HIPAA retention.

- **Right to Amend.** If a patient feels that medical information we have about them is incorrect or incomplete, they may ask us to amend (correct or change) the information. They have the right to request an amendment for as long as the information is kept by or for our Organization.

  - We may deny the request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny a request for amendment if the PHI:

- Was not created by us (unless the originating person or entity that created the information is no longer available to make the amendment);
- Is not part of the medical information (designated record set) kept by or for the Organization;
- Is not part of the information which is available for inspection and copying; or
- Is accurate and complete.

Our Organization Procedures for Amendments to PHI

Include any company-specific procedures if applicable: none

- Use Privacy / Security Combo Forms *'Gs - Request for Patient Rights Form'* and *'Hs - Denial of Amendment or Correction Form'* to document the patient's request and possible denial of the request.
- Record the request *'AAs - ROI Breach Patient's Rights Log'*.
- If the amendment request escalates past a typical request and response, especially if there is a complaint or investigation use Privacy / Security Combo Form *'Bs - HIPAA Security or Privacy Event Reporting Form'* to document the entire process.
- Process the request within 60 days.
- All of the above documentation must be kept for the minimum 6-year HIPAA documentation retention period.

- **Right to an Accounting of Disclosures (AOD).** Patients have the right to request an accounting of disclosures of their PHI by a Covered Entity or its Business Associates. Under HIPAA, a disclosure is a release, transfer, access to, or divulging of information outside of the Practice/Organization. In general, a patient has the right to know who has received his/her health information for reasons other than treatment, payment, and healthcare operations (commonly referred to as "TPO"), or disclosures specifically authorized by the patient. A request for an accounting cannot be earlier than the date the HIPAA Privacy Rule became effective which was April 14, 2003 for most CEs. Examples of disclosures that must be recorded and included in an accounting are: submission of reports required by law, this includes disclosure to Social Services or a protective service agency; responding to judicial or administrative proceedings, disclosures in response to warrants, court orders, subpoenas (unless the individual authorized the disclosure); notifying coroners, medical examiners and organ donation agencies of deaths; for law enforcement purposes, disclosures to report gunshot wounds. There are others, so if you are unsure whether a disclosure should be tracked, check with your supervisor.

  Our Procedures for Accounting of Disclosures

  Include any company-specific procedures if applicable: none

  - Use *'Gs - Request for Patient Rights Form'* to document the patient's request.
  - Record the request in *'AAs - ROI Breach Patient's Rights Log'.*
  - There is no charge for the first AOD request in a 12-month period; a none will be charged for each additional AOD request in the same 12-month period.
  - All of the above documentation must be kept for the minimum 6-year HIPAA documentation retention period.

- **Right to Request Restrictions.** Patients have the right to request a restriction or limitation on the medical information we use or disclose about them for *payment or healthcare operations,* for disclosures to family members or someone who is (or may be) involved in their care and certain other permitted purposes. Covered entities are not required to agree with such requests, but if a

covered entity does agree to the restriction, then the covered entity must abide by that restriction. It is this Organization's policy that we will not agree to any requests to restrict use or access of their medical information for treatment purposes.

Patients also have the right to restrict use and disclosure of protected health information (PHI) if the PHI pertains solely to health care items or services for which the individual or another person on behalf of the individual (other than the health plan) has paid out-of-pocket, in full. We will not accept their request for this type of restriction until there is a zero balance for this item or service.

General advice for restriction requests is to never accept them for treatment purposes and rarely, unless mandated by HIPAA, for payment or operations. Failure to comply with agreed to restrictions can lead to civil liabilities and fines.

Our Procedures for Restrictions

- Use *'Gs - Request for Patient Rights Form'* and *'Hs - Denial of Amendment or Correction Form'* to document the patient's request and possibly denial of the request.
- Record the request in *'AAs - ROI Breach Patient's Rights Log'.*
- Ensure payment for the item or service asking to be restricted carries a zero balance and was paid out-of-pocket, not by insurance. If the item or service is paid out-of-pocket and there is a $0 balance, the restriction request is not optional—it must be accepted and followed.
- Be very careful in agreeing to any restrictions, there are many times when information that was requested for restriction may be present in histories or other encounters which would technically violate the restriction if allowed.
- Set restriction flags or enter notes in the System (and on paper charts that contain the restricted PHI) to ensure workforce members who may be processing requests for disclosure in the future are aware of these restrictions.
- Process the restriction request within 60 days.
- If the restriction request escalates past a typical request and response, especially if there is a complaint or investigation, use *'Bs - HIPAA Security or Privacy Event Reporting Form'* to document the entire process.
- All of the above documentation must be kept for the minimum 6-year HIPAA documentation retention period.

- **Except as provided in [(§2304) authorization delay pursuant to the needs of law enforcement] or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay."**
- **(§2303(a))**
- **Delay:**
- **"The notification required by this act may be delayed if a law enforcement agency determines and advises the entity in writing specifically referencing this section that the notification will impede a criminal or civil investigation. The notification required by this act shall be made after the law enforcement agency determines that it will not compromise theinvestigation or national or homeland security."**
- **Right to Receive Notice of a Breach.** We are required to notify patients by First Class Mail or by email (if the individual has indicated a preference to receive information by email), of any breaches of UNSECURED Protected Health Information as soon as possible, but in any event, no later than (§2304) following the discovery of the breach. Our Organization will investigate any 'event' or incident' where a patient's PHI is known or thought to have been wrongfully disclosed. If it is determined that a breach has occurred both the patient, the Federal and State government will be

notified within notices must be made without resonable delay. It is important to remember that PHI in Systems that are encrypted are not subject to breach (they are considered to be in the 'breach safe harbor'); however HIPAA violations can still occur, therefore all 'events or incidents must be investigated and corrective actions taken, even if a wrongful disclosure is not determined to be a breach.

Our Procedures for Breach Determination and Notification

Include any company-specific procedures if applicable: "[Notice] [m]ay be provided by any of the following methods of notification:
(1) Written notice to the last known home address for the individual.
(2) Telephonic notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance.
(3) E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual.
(4) . . . Substitute notice, if the entity demonstrates one of the following:
(A) The cost of providing notice would exceed $100,000.
(B) The affected class of subject persons to be notified exceeds 175,000.
(C) The entity does not have sufficient contact information."
(§2302)
Substitute notice:
"Substitute notice shall consist of all of the following:
(A) E-mail notice when the entity has an e-mail address for the subject persons.
(B) Conspicuous posting of the notice on the entity's Internet website if the entity maintains one. (C) Notification tomajor Statewide media." (§2302)

- Use the following Privacy / Security Combo Forms to document the incident report, investigation and corrective actions related to investigating, remediating and notifying affected individuals in the case of a breach.
  - Use *'Bs - HIPAA Security or Privacy Event Reporting Form'* to document the patient's report of a security or privacy event.
  - Use *'Cs - Initial Investigation Privacy Security Event'* to document the investigation and corrective actions related to security or privacy events.
  - Use *'Ns - Breach Reporting Form'* to catalog the reportable information about a wrongful disclosure or breach.
  - Use '*S1s - Interim Final Rule Breach Assessment'* for breach determination under the Harm Standard (between September 23, 2009 and September 23, 2103) OR *'Ss - Omnibus Final Rule Breach Assessment'* for breach determination after September

23, 2013 in order to document the factors surrounding our determination of whether a HIPAA Violation is deemed a reportable breach.
    - Use Privacy / Security Combo Policy *'21s - Breach Determination and* Reporting' to guide decisions as to whether an event is determined to a breach; upon determination, report to State and Federal government as necessary.

- Record the request in the *'AAs - ROI Breach Patient's Rights Log'.*

- State enforcement: "A violation of this act shall be deemed to be an unfair or deceptive act or practice in violation of the act of December 17, 1968 (P.L.1224, No.387), known as the Unfair Trade Practices and
- Consumer Protection Law."
- (§2308)
- Private right of action: No.
- "The Office of Attorney General shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this act."
- Reporting timeframes: OCR (Federal Government) must be notified of a breach within 60 days (if over 500 patients). **For breaches that affect fewer than 500 individuals, a covered entity must provide the Secretary with notice annually.** All notifications of breaches occurring in a calendar year must be submitted within 60 days of the end of the calendar year in which the breaches occurred. (§2308).

- All of the above documentation must be kept for the minimum 6-year HIPAA retention period.

- **Right to Request Confidential Communications.** Patients have the right to request that we communicate with them about medical matters in a certain way or at a certain location. For example, they can ask that we only contact them at work or by mail. We will not ask them the reason for their request and will accommodate all reasonable requests.

  Our Procedures for Confidential Communications

  Include any company-specific Procedures if applicable: "[Notice] [m]ay be provided by any of the following methods of notification:
  (1) Written notice to the last known home address for the individual.
  (2) Telephonic notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance.
  (3) E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual.
  (4) . . . Substitute notice, if the entity demonstrates one of the following:
  (A) The cost of providing notice would exceed $100,000.
  (B) The affected class of subject persons to be notified exceeds 175,000.

(C) The entity does not have sufficient contact information."
(§2302)
Substitute notice:
"Substitute notice shall consist of all of the following:
(A) E-mail notice when the entity has an e-mail address for the subject persons.
(B) Conspicuous posting of the notice on the entity's Internet website if the entity maintains one. (C) Notification tomajor Statewide media." (§2302)

- Use *'Gs - Request for Patient Rights Form'* to document the patient's request.
- Record the request in the *'AAs - ROI Breach Patient's Rights Log'.*

- **Right to a Copy of Our Notice of Privacy Practices (NPP).** If the patient or another party requests a copy of our NPP, be sure to provide it to them in whatever form they wish.

- **Handling Security or Privacy Complaints.** If a patient, another party or one of the Organization's workforce members, Business Associates or contractors believes that privacy rights have been violated or that a HIPAA violation has occurred, they may file a complaint with the Organization or with the Secretary of the Department of Health and Human Services at the website URL shown below. Always advise the party of their rights and be supportive. Refer to *'20s - Handling Privacy Complaints, Internal & External'* for guidance.

http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html

Section B: Security

This section of this guide is intended to give a general overview of the security compliance measures undertaken by this Organization. This summary *is not* intended to be an exhaustive list, rather an overview of the more common safeguards we employ. Please refer to our detailed polices, any written procedures and Risk Assessments for more information and statutory language or specific rules.

1. **Risk Assessment**
   Risk Assessment to be updated routinely as the Organization's safeguards materially change, but not less than yearly.
   Company Risk Assessment Specifics: Assesment to be conducted during quality management meetings

2. **Workforce Clearance**
   Company Workforce Specifics: none

3. **Workforce Termination**
   Workforce members who are terminated will have their access to computer systems and networks removed immediately according to policy timeframes and procedures.
   Company Termination Specifics: Upon violation a review will be conducted the staff member will be put on probation or terminated.

4. **Access to PHI**
   All appropriate access to PHI is secured through the use of passwords which are changed routinely; of appropriate strength and unique to each user. All access to PHI is through formal

logon. Remote access is via secured data in transit and no data is stored on mobile devices.
Company PHI Access Specifics: Staff members will abide by least amount of PHI necessary to do their jobs and be assigned specific log ins to access their clients

5. **Password Management**
   Passwords expire and must be changed every 6 months. Use of more secure passwords, i.e. multiple digit letter number combinations is required
   Company Password Specifics: to be assigned

6. **Auto Log-off**
   Users are logged off of PCs and Servers after periods of inactivity.
   Company Logoff Specifics: will be logged off after a minute of inactivity

7. **Back-up and Restoration**
   Multiple levels of routine and remote back-ups are maintained. They are tested for restoration integrity and are encrypted data at rest and in transit.
   Company Backup Specifics: Third party company to back up offsite daily

8. **Encryption for Breach Safe Harbor**
   Company Safe Harbor Specifics: For establishing own notification method: Yes.
   "An entity that maintains its own notification procedures as part
   of an information
   privacy or security
   policy for the treatment of personal information and is consistent with the notice requirements of this act shall be deemed to be in compliance with the notification
   requirements of this
   act if it notifies
   subject persons in
   accordance with its
   policies in the event
   of a breach of
   security of the
   system."
   (§2307(a))
   For following interagency guidelines: Yes.
   "(1) A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this act.
   (2) An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures or guidelines established by the entity's primary or functional Federal regulator shall be in compliance with this act."
   (§2307(b))

9. **Malware Prevention –** Anti-virus, firewall(s), intrusion monitoring, detection and prevention and similar safeguards are all up to date and continually maintained**.**

10. **Physical Security –** The Organization has locks, alarms and segregated records and computers / monitors for patient areas, as practical. Maintenance records for all physical security items are kept for the 6-year HIPAA documentation retention period**.**

11. **Media and Devices**
    Company Media and Device Specifics: Yearly security privacy and security training for HIPAA

12. **Audit Controls –** Google Documents maintains an audit log of all user activities which is monitored at least quarterly for inappropriate access, use or disclosure. We also monitor error and technical logs for inappropriate activity on a routine basis**.**

13. **Security and Privacy Training**
    Workforce members are trained at new hire, at least annually thereafter and whenever there are material changes to the privacy / security rules or job roles which require a different level of training. Security and privacy reminders are discussed at staff meetings and other opportunities. Tests and documentation of the training is kept for the 6-year HIPAA documentation retention period.
    Company Training Specifics: Yearly security privacy and security training for HIPAA

