127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Access & Denial for PHI | | | Policy # | 701 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 3 | |
| Policy Section | HIPAA Policies | | | | |

**PURPOSE:**

To assure compliance that supports HIPAA regulations.

**POLICY:**

It is the policy of Ponderosa Family Care to secure and maintain the medical records of each and every patient receiving clinic services.

**PROCEDURE:**

1. The access and denial process is managed by the Practice Administrator .

2. Patients have a right to inspect and receive a copy, at their expense, of the PHI in their designated record set. Exceptions to this include:
   A. Psychotherapy notes, but not a summary of these.
   B. Information compiled in anticipation of or use in a civil, criminal, or administrative action or proceeding.
   C. PHI subject to the Clinical Laboratory Improvements Amendments (CLIA) of 1988.
   D. Employee Assistance Program (EAP) records, which are not part of the record set, but may be requested separately.

3. A patient has the right to inspect, or receive copies of PHI about the patient in a designated record set for as long as the PHI is maintained in the designated record set.

4. If the clinic does not maintain the PHI that is the subject of the patient's request for access, and the clinic knows where the requested information is maintained, the clinic must inform the patient where to direct the request for access.

5. The patient must make the request in writing.

6. If access is granted, in whole or in part, the clinic must comply with the following requirements:
   A. The clinic must provide the patient access to his/her PHI in the designated record sets, including inspection or receiving a copy, or both. If the same PHI that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the clinic need only produce the PHI once in response to a request for access.

B. The clinic must provide the patient with access to the PHI in the form or format requested by the patient, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by both parties.
C. The clinic may provide the patient with a summary of the PHI requested, in lieu of providing access to the PHI or may provide an explanation of the PHI to which access has been provided, if:
   i. The patient agrees in advance to such a summary or explanation; and
   ii. The patient agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.
D. The clinic must provide the access as requested by the patient in a timely manner, including arranging with the patient for a convenient time and place to inspect or receive a copy of the PHI, or mailing the copy of the PHI at the patient's request. The clinic may discuss the scope, format, and other aspects of the request for access with the patient as necessary to facilitate the timely provision of access.
E. If the patient requests a copy of the PHI or agrees to a summary or explanation of such information, the clinic may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:
   i. Copying, including the cost of supplies for and labor of copying the PHI requested.
   ii. Postage, if the patient has requested the copy, summary, or the explanation mailed.
   iii. Preparing an explanation or summary of the PHI, if agreed to by the patient.

7. The clinic must allow a patient to request access to inspect or receive a copy of PHI maintained in their designated record set. However, the clinic may deny a patient's request without providing an opportunity for review when:
   A. An exception detailed above in the policy exists.
   B. The clinic is acting under the direction of a correctional institution and the prisoner's request to obtain a copy of PHI would jeopardize the patient, other prisoners, or the safety of any officer, employee, or other person at the correctional institution, or a person responsible for transporting the prisoner.
   C. The PHI was obtained from someone other than the clinic under a promise of confidentiality and access would likely reveal the source of the information.
   D. The clinic may also deny a patient access for other reasons, provided that the patient is given a right to have such denials reviewed under the following circumstances.
      i. The ordering physician has determined that the access is likely to endanger the life or physical safety of the patient or another person.
      ii. The PHI makes reference to another person who is not a healthcare provider, and the referring physician has determined that the access requested is likely to cause substantial harm to the patient or another person.
   E. If access is denied on the grounds permitted above, the patient has the right to have the denial reviewed by a licensed health professional, designated or appointed by the clinic to act as a reviewing official, and who did not participate in the original decision to deny. The clinic must provide or deny access in accordance with the determination of the reviewing official.
   F. If the clinic denies access, in whole or in part, to PHI, the clinic must comply with the following requirements:

i. The clinic must, to the extent possible, give the patient access to any other PHI requested, after excluding the PHI to which the clinic denied access.
ii. The clinic must provide a timely, written denial to the patient, in plain language within 30 days and containing:
    a) The basis for the denial.
    b) If applicable, a statement of the patient's review rights, including a description of how the patient may exercise such review rights.
    c) A description of how the patient may complain to the clinic.
iii. If the patient has requested a review of a denial, the clinic must designate or appoint a licensed healthcare professional who was not directly involved in the decision to deny access. The clinic must promptly refer a request for review to such licensed healthcare professional. The licensed healthcare professional must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards. The clinic must promptly provide written notice to the patient of the findings and take other action as required by this section to carry out the licensed healthcare professional's determination.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Accounting of Disclosure of PHI | | | Policy # | 702 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 3 | |
| Policy Section | HIPAA Policies | | | | |

**PURPOSE:**

To assure compliance with a patient's right to obtain an accounting of disclosures of protected health information (PHI).

Background: Patients may request an accounting of disclosures of PHI for a period of up to six (6) years prior to the date of the request. In addition, a patient may request an accounting of such information for a shorter period of time, such as one (1) year.

**POLICY:**

It is the policy of Ponderosa Family Care to maintain a history of disclosures of PHI and to implement and maintain procedures to receive, process, and approve or deny all patient requests for an accounting of disclosures of their PHI.

**PROCEDURE:**

1. The clinic must account for all disclosures of PHI, except for disclosures made for Treatment, Payment or health care Operations (TPO) or pursuant to a patient authorization. Additionally, the clinic will not account for disclosures made to referring physicians (physicians requesting consults or specialty procedures). Disclosures to referring physicians fall within the TPO exception.

2. The clinic must provide the individual with a written accounting that meets the following requirements:

   A. Except as otherwise provided, the accounting must include disclosures of PHI that occurred during the six years (or shorter time period if requested) prior to the date of the request. This includes disclosures to and by business associates for purposes other than TPO.
   B. The accounting for each disclosure must include:
      i. The date of the disclosure.
      ii. The name of the entity or person who received the PHI and, if known, the address of such entity or person.
      iii. A brief description of the PHI disclosed.
      iv. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or in lieu of such statement a copy of a written request for a disclosure if any.

C. If the clinic has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting may, with respect to such multiple disclosures, provide:
   i. The information required above.
   ii. The frequency, periodicity, or number of the disclosures made during the accounting period.
   iii. The date of the last such disclosure during the accounting period.

3. Disclosures for research purposes must be accounted for unless an authorization has been obtained from the individual. For research disclosures involving less than 50 individuals the clinic must account for the disclosure in accordance with the above requirements.

4. For larger research disclosures (more than 50 individuals) the clinic may provide a summary list of all protocols for which the patient's PHI may have been disclosed for research pursuant to a waiver of authorization. The summary list must provide:

   A. The name of the protocol or other research activity.
   B. A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records.
   C. A brief description of the type of PHI that was disclosed.
   D. The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period.
   E. The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed.
   F. A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

5. The clinic must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows:

   A. Provide the individual with the accounting request
   B. If the clinic is unable to provide the accounting within the time required above, the clinic may extend the time to provide the accounting by no more than 30 days, provided that:
      i. The clinic, within the time limit of 60 days, provides the individual with a written statement of the reasons for the delay and the date by which the clinic will provide the accounting.
      ii. The clinic may have only one such extension of time for action on a request for an accounting.

6. The clinic must provide the first accounting to an individual in any 12-month period without charge. The clinic may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12-month period, provided that the clinic informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

7 Clinic personnel need to account for disclosures of PHI by documenting any such disclosures. The office coordinator or their designee will be responsible for documenting accounting disclosures

8. The Practice Administrator will be responsible for receiving and processing requests for an accounting of disclosures.
   A. The Practice Administrator must document and maintain a copy of the following:
      i. The required information to be included in an accounting of disclosures, as outlined in this policy.
      ii. The written accounting that is provided to the individual requesting an accounting of disclosures.

9. The clinic must temporarily suspend an individual's right to receive an accounting of disclosures made to a health oversight agency or law enforcement official, if such agency or official provides the clinic with a written statement that such an accounting to the individual is reasonably likely to impede agency activity. The written statement must specify the time for which such a suspension is required.

10. If the agency or official suspends an individual's right to receive an accounting of disclosures and the statement is made orally, the clinic must:
    A. Document the statement, including the identity of the agency or official making the statement.
    B. Temporarily suspend the individual's right to an accounting of disclosures subject to the statement.
    C. Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement from the suspending agency or official is submitted during the time period.

11. The clinic is not required to account for the following disclosures:
    A. To carry out TPO.
    B. To individuals requesting their own PHI.
    C. Incidental use or disclosure made during an otherwise permitted or required disclosure.
    D. Pursuant to an authorization.
    E. For national security or intelligence purposes.
    F. To correctional institutions or law enforcement officials.
    G. As part of a limited data set.

## Accounting of Disclosure of Protected Health Information.

**Patient Name:**_____ **MR#**_____ **Date:**_____

There are some situations in which Ponderosa Family Care is required or permitted by law to disclose your health information to persons outside of our office. In response to your request, we are providing you with this accounting of disclosures we have made of your information.

- ☐ We have made no disclosures of your health information that require an accounting.
- ☐ We have made the following disclosures:

| Disclosure Date | Recipient Name | Recipient Address | Description of PHI Disclosure | Purpose of Disclosure | Frequency of Disclosure/ Date of Last Disclosure |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

This accounting does not include disclosures we have made to carry out treatment, payment or health care operations or disclosures you have specifically authorized. It also does not include any disclosures the law exempts from our accounting requirements. If you have questions about this accounting, please contact Ponderosa Family Care.

**REQUEST FOR AN ACCOUNTING OF DISCLOSURES**

DATE OF REQUEST:_____

PATIENT NAME:_____ DOB:_____

PATIENT ADDRESS:_____

SSN:_____

ADDRESS TO SEND DISCLOSURE ACCOUNTING (if different from above):

I would like an accounting of all disclosures for the following time frame (please note the maximum time frame that can be requested is six years prior to the date of the request, but not before _____.

From: _____ To:_____

**FEES**

| | |
|---|---|
| First request in a 12-month period | Free |
| Subsequent Requests | $5.00 |
| The fee for this request will be: | _____ |

I understand that there is a fee for this accounting and wish to proceed. I also understand that the accounting will be provided to me within 60 days unless I am notified in writing that an extension of up to 30 days is needed.

_____ _____

Signature of Patient or Legal Representative Date

**For Clinic Use Only:**

Date Received:_____ Date Sent:_____

Extension Requested: ☐ NO ☐ Yes Reason:_____

Patient notified in writing on this date: _____

Copy of Verification of Identity of patient and/or legal representative obtained/filed

☐ NO ☐ Yes

Staff member processing request:_____

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Appropriate Access to PHI by Workforce | | | Policy # | 703 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 2 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

To define the policy related to timely and appropriate access to patient information along with PHI confidentiality. Each user is ultimately responsible for adhering to this policy. Users must only access/view the minimum set of PHI that they have a legitimate "need to know," regardless of the extent of access provided.

## POLICY:

Appropriate access to clinical information is defined as providing a user timely access to patient-specific information, which is necessary to perform his/her professional responsibilities. Access will be granted for an individual to provide and/or support quality patient care processes, as defined by an individual's professional responsibilities to the patient and the facility. All department management, administration, and members of the Ponderosa Family Care's executive committee are responsible for ensuring that this policy is applied to all individuals using PHI.

## PROCEDURE:

This policy embraces the following principles related to the collection, processing, maintenance, and storage of patient information.

1. Workforce members will access, use, collect, dispose, process, view, maintain, and store patient's clinical and financial information in an honest, ethical, and confidential manner.

2. The access, use, collection, processing, viewing, maintenance, and storage of patient information will be done in such a manner that, at a minimum, it meets all applicable Federal and State Laws, Rules, Regulations, and Accreditation Standards.

3. Each department within the Ponderosa Family Care must provide support to effectively maintain patient information in a confidential manner.

4. Access to patient information will be limited to individuals with a legitimate "need to know" in order to effectively perform their specific job duties and responsibilities. Minimum Necessary Use of PHI principals is also applied. User roles and related permissions are defined and managed within all computer systems that contain PHI (ePHI).

5. Workforce member access to PHI will be granted after execution of appropriate confidentiality statement by the workforce member.

6. Job descriptions will address what PHI is accessible by which job roles.

7. Access to PHI will be according to specific written policies and procedures.

8. All workforce members must conform to security policies, i.e., not sharing access credentials, to help protect PHI.

**Protocol for Breach of PHI Confidentiality (Privacy):**

Breach of Privacy will be handled in accordance with administrative policies.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Access Controls | | | Policy # | 704a |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 2 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

To implement the technical procedures for electronic information systems that maintain electronic protected health information (ePHI) to allow access only to those persons or software programs that have been granted access rights as specified in section 164.308 of HIPAA law.

## POLICY:

It is the policy of Ponderosa Family Care to implement reasonable and appropriate measures to (1) limit access to ePHI only to those persons or automated processes that have been granted access rights based on their required functions and (2) prevent those who have not been granted those rights from obtaining access to ePHI.

## PROCEDURE:

This HIPAA Standard includes four (4) Implementation Specifications:

- Unique user identification (*required*)
- Emergency access procedure (*required*)
- Automatic logoff (*addressable*)
- Encryption and decryption (*addressable*)

To ensure that only authorized users or software programs are given access to EPHI, the following measures shall be implemented:

1. Unique User Identification.

   (a) All users shall be assigned a unique name and/or number which will allow for the identification and tracking of the user's access to EPHI.

   (b) Access to systems containing EPHI must be limited based on the user's identification, role, or context of a particular request.

   (c) Access control must be modified and/or terminated when an individual's role within the organization changes or when an individual is no longer a member of Radiology Clinic's Workforce.

2. Emergency Access Procedure.

(a) Mechanisms must be developed to access all original EPHI (that is, PHI that is not a copy of information stored in the paper medical file) during emergencies, such as power outages.

3. Automatic Logoff.

(a) All applications at unattended workstations must either be turned off or secured by a password, if the user plans to be away from the workstation.

(b) All applications at workstations must have an automatic log-off capability after inactivity.

4. Encryption and Decryption.

(a) The use of mechanisms to encrypt and decrypt EPHI shall be assessed on a case-by-case basis in order to prevent unauthorized access. The need to incorporate encryption and decryption mechanisms will increase in the event the EPHI is sent to a third-party electronically.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Audit Controls | | | Policy # | 704b |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 1 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

This policy is designed to implement the Audit Controls Standard (§164.312(b)) of the HIPAA Security Rule This Standard is *required.*

## POLICY:

It is the policy of Ponderosa Family Care to support security management activities designed to detect potential security incidents by implementing hardware, software, and/or procedural mechanisms that will record and examine information systems activity in information systems that contain or use ePHI.

## PROCEDURE:

To ensure that proper audit controls are in place, the following measures will be implemented:

(1) All network log-on successes and failures must be logged.

(2) Any electronic information systems or software containing EPHI that have the ability to monitor an individual's activity must be activated.

(3) All audit logs and records must be kept for a minimum of ninety (90) days.

This will be maintained by the EMR vendor, and available upon request or need.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Breach Determination and Reporting | | | Policy # | 705 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 6 | |
| Policy Section | HIPAA Policies | | | | |

**PURPOSE:**

The purpose of this policy is to establish procedures for determining the need for breach notification, as well as for providing notification to appropriate parties in the event of a breach of an individuals' unsecured protected health information (PHI).

Background:
The HIPAA Breach Notification Rule, 45 CFR §§164.400-414, requires HIPAA covered entities and their business associates to provide notification following a "breach" of "unsecured" protected health information.

**Definition of "Breach"**
A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information 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 protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

**Exceptions to the definition of "breach"**
There are three exceptions to the definition of "breach."

1. The first exception applies to the unintentional acquisition, access, or use of protected health information 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.
2. The second exception applies to the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity

participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.

3. The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

**Breach Presumed.** An acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rules is presumed to be a Breach unless we, or our Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following four (4) factors:

a) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

b) The unauthorized person who used the PHI or to whom the disclosure was made;

c) Whether the PHI was actually acquired or viewed;

d) The extent to which the Medical the risks to the PHI has been mitigated.

**"Unsecured" Protected Health Information**
Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in HIPAA guidance.

**Breach Notification Requirements**
Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate,

Covered entities and business associates must only provide the required notifications if the breach involved "unsecured protected health information".

**POLICY:**

NAME OF CLINIC will comply with applicable law in determining the need for Breach notification, as well as for providing notification to appropriate parties in the event of a breach of an individual's unsecured PHI.

**PROCEDURE:**

**1. Reporting Suspected Breaches; Investigation**

All employees, medical staff, volunteers, temporary workers, independent contractors, and consultants ("workforce members") must immediately report any suspected Breach to the Privacy

Officer within forty-eight (48) hours of becoming aware of such event. Reports will be submitted via the HIPAA Problem/Concern Report.

The Privacy Officer shall be responsible for investigating the facts and circumstances of a suspected Breach, and for determining whether a reportable Breach has, in fact, occurred, via a risk assessment. At the conclusion of the investigation, the Privacy Officer will be responsible for documenting the investigation's outcome, including whether a Breach notification is or is not determined to be necessary.

## 2. Notification Process

**Individual Notification**. Following the discovery of a Breach, the Privacy Officer will notify each individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such Breach ("Individual Notification").

Except in cases of a Law Enforcement Delay, an Individual Notification shall be provided without unreasonable delay, and in no case later than sixty (60) calendar days after the discovery of a Breach.

Each Individual Notification will be in plain language and will include, to the extent possible, 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. However, this description should not include the actual PHI that was Breached and/or include any sensitive information;

c) Any steps the affected individual should take to protect himself/herself from potential harm resulting from the Breach;

d) A brief description of what we are doing to investigate the Breach, to mitigate harm to the individual, and to protect against any further Breaches; and

e) Contact procedures for the individual to ask questions or learn additional information about the Breach, which shall include a toll-free telephone number, an E-mail address, Website, or postal address.

The individual notification must be provided in written form, by first class mail, to the individual at the last known address of the individual, or by E-mail if the individual has agreed to receive such notices electronically. The notification may be provided in one or more mailings as information becomes available. As appropriate and permitted by the Privacy Rules, Individual Notification may be sent to an individual's authorized personal representative.

If we have insufficient or out-of-date contact information for 10 or more individuals, we must provide substitute individual notice by either posting the notice on our web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. We must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If we have insufficient contact information for fewer than 10 individuals, we may provide substitute notice by an alternative form of written notice, by telephone, or other means.

In any case deemed by us to require urgency because of possible imminent misuse of Unsecured PHI, we may provide information to the affected individual(s) by telephone or other means, as appropriate. However, this initial contact shall be followed by written Individual Notification to the affected individual(s).

**Media Notice.** In the event we experience a Breach affecting more than 500 individual-residents of a single State or jurisdiction, in addition to notifying the affected individuals, we must provide notice (*e.g.,* a press release) to prominent media outlets serving the State or jurisdiction ("Media Notice"). Except in cases of a Law Enforcement Delay, the Media Notice shall be provided without unreasonable delay, and in no case later than sixty (60) days following the discovery of a Breach and will include the same information required for an Individual Notification.

**Department of Health and Human Services (DHHS) Notice.** In addition to notifying affected individuals and the media of a Breach, we must notify the Secretary of DHHS of a Breach as follows:

- For Breaches Affecting More than 500 Individuals. In the event a Breach affects 500 or more individuals, we must, except in cases of a Law Enforcement Delay, provide the notification without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach. We must provide Individual Notification at this same time.

- For Breaches Affecting Less than 500 Individuals - For Breaches involving less than 500 individuals, we must maintain a log or other documentation of such Breaches and, not later than 60 days after the end of each calendar year, provide the notification of such Breaches discovered during the preceding calendar year.

Notifications described above may be completed by visiting the HHS website and electronically submitting a breach report form.

**Law Enforcement Notification Delay**. Notification required by HIPAA may be delayed if a law enforcement official states to us that notification, notice, or posting would impede a criminal investigation or cause damage to national security ("Law Enforcement Delay").

a) If the statement is in writing and specifies the time for which a delay is required, we may delay such notification, notice or posting for the time period specified by the office.
b) If the statement is made orally, we shall document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily, but no longer than thirty (30) days from the date of the oral statement, unless a written statement meeting the requirements in Section 4(d)1. above is submitted by the official during that time.

The Privacy Officer shall be responsible for maintaining and retaining copies of any Breach notifications to individuals, the media, and Secretary of HHS as well as any Law Enforcement Delay statements. Such documentation shall be maintained and retained in accordance with our HIPAA Compliance Plan documentation requirements and standards.

## 3. HIPAA Business Associates

Our HIPAA Business Associates must notify us in the event they discover or suspect any Breach. A Breach will be treated as discovered by a Business Associate as of the first day on which such Breach is known to the Business Associate or, by exercising reasonable diligence, would have been known to the Business Associate.

A Business Associate shall be deemed to have knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer, or other agent of the Business Associate. Such notifications shall be made in accordance with the terms of the HIPAA Business Associate Agreement between the parties and/or as otherwise directed by us.

## 4. Mitigation; Administrative Obligations

Mitigation. We must take prompt corrective action to mitigate and cure, if feasible, any harmful effect that is known to us resulting from a Breach of Unsecured PHI.

Training and Education: Training and education on this policy shall be provided to workforce members and associates as appropriate and necessary for such individuals to carry out their respective duties and responsibilities to our organization.

Complaints. The Privacy Officer will be responsible for implementing a process and procedure for addressing complaints concerning the handling of a Breach.

Sanctions. Failure to comply with this policy may result in disciplinary action, including possible termination.

## ATTACHMENTS:

HIPAA Problem/Concern Report

****CONFIDENTIAL****

## Ponderosa Family Care

## HIPAA Problem/Concern Report

The HIPAA Problem/Concern Report form is to be used by members of our Workforce to report their good faith belief of violations of the Privacy Rules, Security Rules, our HIPAA Compliance Plan, applicable law, as well as other ethical standards regarding the protection, privacy, and security of protected health information. **We will take every measure to ensure the confidentiality of the information outlined below. However, there may be circumstances where disclosure of this information may become necessary.**

1. **Your Name:** _____

2. **Date of Incident:** _____ **Date of Discovery:** _____

3. **Time:** _____ AM or PM (*circle one*)

4. **Your Job Title:** _____

5. **Department:** _____

6. **Detailed description of the problem/concern/possible violation** *Include dates, location(s) of incident, names of persons involved, general description of the health information disclosed, means of violation (phone, fax, email, virus, theft, etc.), and duration of event:* Please continue on back if more space is needed.

_____
_____
_____
_____
_____
_____

7. **If information was received outside of Ponderosa Family Care, was it destroyed, and if so by whom?**

_____

8. **How did you become aware of the problem?** _____
_____
_____
_____

9. **Was information shared with anyone inside or outside the clinic, and if so, with whom?**

_____

10. **Others with knowledge of the problem/concern/possible violation:** _____

This report was received by the Director of Privacy & Compliance/Privacy Officer/Security Officer on:

_____

_____ _____

Signature of Director of Privacy & Compliance/Privacy Officer/Security Officer Date

---

***This Section For Administrative Use Only***

---

***The following information is to be completed after an investigation is conducted.***

Date Investigation Initiated: _____

Problem/Concern/Violation Valid? Yes OR No (*circle one*)

General Description of Problem/Concern/Violation Found: _____

_____

_____

_____

_____

Action taken: _____

_____

_____

Date Investigation Closed: _____

Approved: _____

Signature of Director of Privacy & Compliance/Privacy Officer/Security Officer Date

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Business Associates Agreement | | | Policy # | 706 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 2 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

To assure compliance for contracts with business associates.

## POLICY:

It is the policy of Ponderosa Family Care to secure and maintain the medical records of each and every patient receiving clinic services.

## PROCEDURE:

1. A business associate is any person or organization that performs or helps to perform any function or activity that involves the use or disclosure of protected health information on behalf of the clinic and is not an employee or member of the clinic's workforce.

2. Functions or activities are defined as: legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the clinic, where the provision of the service involves the disclosure of individually identifiable health information from the clinic, or another business associate.

3. The business associate contract must include provisions that have the following satisfactory assurances:
   A. Identify the uses and disclosures of PHI permitted under the business associate agreement or initial client contract.
   B. Permit the business associate to use or disclose the information only as permitted under the privacy standards.
   C. Restrict use and disclosure of the PHI that the business associate creates or receives to those that are specified in the business associate agreement or initial client contract.
   D. Call on the business associate to establish and use safeguards to prevent use and disclosure other than as provided for in the contract with the clinic.
   E. Provide for reporting to the clinic of any use or disclosure of PHI not provided for under the business associate's contract.
   F. Require the business associate to apply the same restrictions and conditions on use and disclosure of PHI to the agents and subcontractors to whom it forwards the PHI.
   G. Amend any PHI that it receives when asked to do as requested by the Practice Administrator.
   H. Make available to the clinic information needed to account for uses and disclosures of PHI.

I. Make internal Clinics, books, and records that are related to the use and disclosure of PHI available to the Department of Health and Human Services for purposes of determining compliance with the privacy standards.
J. Return, if feasible all PHI to the clinic upon termination of the contract, and destroy any copies of such information. When return and/or destruction of PHI is not possible, the business associate will extend contractual protections to the use and disclosure of the information for the purposes that make its return or destruction impossible.
K. Provide for termination of the contract if the business associate violates these contractual provisions.

4. If an employee becomes aware of activities by the business associate that violate its contractual obligations, it must be reported to the Practice Administrator.

5. When the Practice Administrator is notified that a business associate has violated a contractual provision related to the privacy of PHI, the Practice Administrator must implement the following procedure to correct the violation:
   A. The Practice Administrator will contact the business associate and determine whether a contractual provision has been violated.
   B. If a contract provision has been violated, the Practice Administrator will identify steps to be taken by the contractor that will enable the business associate to comply with its contractual obligations.
   C. The Practice Administrator will review the corrective action steps with the business associate and determine whether those steps or other measures suggested by the business associate will correct the violation. If an agreement can be reached, the corrective measures will be summarized in writing and sent to the business associate.
   D. Practice Administrator will monitor the implementation of the corrective action measures by periodically contacting the business associate. The Practice Administrator may discontinue monitoring the contract after receiving adequate assurances that the corrective measures have been implemented and that the contract provisions will be complied within the future.

6. If it is not possible to develop an acceptable corrective action plan, the Practice Administrator will contact the owner to potentially terminate the contract.

7. See attached Business Associates Agreement (BAA).

**EFFECTIVE DATE: DATE**

**BUSINESS ASSOCIATE AGREEMENT**

**FOR HEALTH CARE PROVIDERS**

**This Agreement is entered into by and between NAME OF CLINIC herein referred to as the *Health Care Provider* and NAME OF OTHER ENTITY, herein referred to as the *Business Associate*, to set forth the terms and conditions under which "protected health information," as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Regulations enacted there under, created or received by the *Business Associate* on behalf of the *Health Care Provider* may be used or disclosed.**
**This Agreement shall commence on DATE and the obligations herein shall continue in effect so long as the *Business Associate* uses, discloses, creates or otherwise possesses any protected health information created or received on behalf of the *Health Care Provider* and until all protected health information created or received by *Business Associate* on behalf of *Health Care Provider* is destroyed or returned to the *Health Care Provider* pursuant to Paragraph 15 herein.**

1. **The *Health Care Provider* and *Business Associate* hereby agree that the *Business Associate* shall be permitted to use and/or disclose protected health information created or received on behalf of the *Health Care Provider* for the following purpose(s): To act as deeming entity.**

2. **The *Business Associate* may use and disclose protected health information created or received by the *Business Associate* on behalf of the *Health Care Provider* if necessary for the proper management and administration of the *Business Associate* or to carry out the *Business Associate's* legal responsibilities, provided that any disclosure is:**
   a. **Require by law, or**
   b. **The *Business Associate* obtains reasonable assurances from the person to whom the protected health information is disclosed that (i) the protected health information will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and (ii) the *Business Associate* will be notified of any instances of which the person is aware in which the confidentiality of the information is breached.**

3. **The *Business Associate* hereby agrees to maintain the security and privacy of all protected health information in a manner consistent with state and federal laws and regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Regulations there under, and all other applicable law.**

4. **The *Business Associate* further agrees not to use or disclose protect health information except as expressly permitted by the Agreement, applicable law, or for the purpose of managing the *Business Associate's* own internal business processes consistent with Paragraph 2 herein.**

5. **The *Business Associate* shall not disclose protected health information to any member of its workforce unless the *Business Associate* has advised such person of the *Business Associate's* privacy and security obligations under this Agreement, including the consequences for violation of such obligations. The *Business Associate* shall take appropriate disciplinary action against any member of its workforce who uses or disclosed protected health information in violations of this Agreement and applicable law.**

6. **The *Business Associate* shall not disclose protected health information created or receive by the *Business Associate* on behalf of *Health Care Provider* to a person, including any agent or subcontractor of the *Business Associate* but not including a member of the *Business Associate's* own workforce, until such person agrees in writing to be bound by the provisions of this Agreement and applicable state or federal law.**
7. **The *Business Associate* agrees to use appropriate safeguards to prevent use or disclosure of protected health information not permitted by this Agreement or applicable law.**

8. **The *Business Associate* agrees to maintain a record of all disclosures of protected health information, including disclosures not made for the purposes of this Agreement. Such record shall include the date of the disclosure, the name and, if known, the address of the recipient of the protected health information, the name of the individual who is the subject of the protected health information, a brief description of the protected health information disclosed and the purpose of the disclosure. The *Business Associate* shall make such record available to an individual who is the subject of such information or the *Health Care Provider* within five (5) days of a request and shall include disclosures made on or after the date which is six (6) years prior to the request.**

9. **The *Business Associate* agrees to report to the *Health Care Provider* any unauthorized use or disclosure of protected health information by the *Business Associate* or its workforce or subcontractors and the remedial action taken or proposed to be taken with respect to such use or disclosure.**

10. **The *Business Associate* agrees to make its internal practices, books, and records relating to the use and disclosure of protected health information receive from the *Health Care Provider*, or created or received by the *Business Associate* on behalf of the *Health Care Provider*, available to the Secretary of the United States Department of Health and Human Services, for purposes of determining the Covered Entity's compliance with HIPAA.**

11. **Within thirty (30) days of a written request by the *Health Care Provider*, *Business Associate* shall allow a person who is the subject of protected health information, such person's legal representative, or the *Health Care Provider* to have access to and to copy such person's protected health information maintained by the *Business Associate*. The *Business Associate* shall provide protected health information in the format requested by such person, legal representative, or practitioner unless it is not readily producible in such format, in which case it shall be produced in standard hard copy format.**

12. **The *Business Associate* agrees to amend, pursuant to a request by the *Health Care Provider*, protected health information maintained and created or received by the *Business Associate***

**on behalf of Practitioner. The *Business Associate* further agrees to complete such amendment within thirty- (30) days of a written request by the *Health Care Provider*, and to make such amendment as directed by the *Health Care Provider*.**

13. **The *Health Care Provider* may immediately terminate this Agreement and related agreements if the *Health Care Provider* determines that the *Business Associate* has breached a material term of this Agreement. Alternatively, the *Health Care Provider* may choose to: (1) provide the *Business Associate* with ten (10) days written notice of the existence of an alleged material breach; and (ii) afford the *Business Associate* an opportunity to cure said alleged material breach to the satisfaction of the *Health Care Provider* within ten (10) days. The *Business Associate's* failure to cure shall be grounds for immediate determination of this Agreement. The *Health Care Provider's* remedies under this Agreement are cumulative, and the exercise of any remedy shall not preclude the exercise of any other.**

14. **Upon termination of this Agreement, the *Business Associate* shall return or destroy all protected health information received from the *Health Care Provider*, or created or received by the *Business Associate* on behalf of the *Health Care Provider* and that the *Business Associate* maintains in any form, and shall retain no copies of such information. If the parties mutually agree that return or destruction of protected health information is not feasible, the *Business Associate* shall continue to maintain the security and privacy of such protected health information in a manner consistent with the obligations of this Agreement and as required by applicable law, and shall limit further use of the information to those purposes that make the return or destruction of the information infeasible. The duties hereunder to maintain the security and privacy of protected health information shall survive the discontinuance of this Agreement.**

15. **The *Health Care Provider* may amend this Agreement by providing ten (10) days prior written notice to the *Business Associate* in order to maintain compliance with state or federal law. Such amendment shall be binding upon the *Business Associate* at the end of the ten (10) day period and shall not require the consent of the *Business Associate*. The *Business Associate* may elect to discontinue the Agreement within the ten (10) day period, but the *Business Associate's* duties hereunder to maintain the security and privacy of PROTECTED HEALTH INFORMATION shall survive such discontinuance. The *Health Care Provider* and the *Business Associate* may otherwise amend this Agreement by mutual written agreement.**

16. **The Business Associate shall, to the fullest extent permitted by law, protect, defend, indemnify and hold harmless the Health Care Provider and his/her respective employees, directors, and agents (Indemnities) from and against any and all losses, costs, claims, penalties, fines, demands, liabilities, legal actions, judgments, and expenses of every kind (including reasonable attorney fees, including at trial and on appeal) asserted or imposed against any Indemnities arising out of the acts or omissions of the Business Associate or any subcontractor of or consultant of the Business Associate or any of the Business Associate's employees, directors, or agents related to the performance or nonperformance of this Agreement.**

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Confidentiality | | | Policy # | 707 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 1 | |
| Policy Section | HIPAA Policies | | | | |

**PURPOSE:**

To ensure patient's right to privacy and confidentiality of patient information consistent with State and Federal laws.

**POLICY:**

It is the policy of Ponderosa Family Care to secure and maintain the medical records of each and every patient receiving clinic services.

**PROCEDURE:**

1. A request to release information will be honored if signed by the patient or legal guardian.

2. Information will be released without consent **only** if there is suspected child /elder abuse as required by State law.

3. In cases of emergency, only the physician or mid-level provider will take requests for release of information to medical personnel over the telephone.
   A. A request will be made for a signed consent to be sent to the clinic, if possible.
   B. If signed consent is not possible at this time, the patient will be asked to sign a release at the next visit to the clinic.
   C. Any information given over the telephone will be documented in the chart.

4. Patient records will be transferred following authorization by the patient or legal guardian. See *Authorization For Use and Disclosure of Protected Health Care Information* form.

5. If there is a breach of confidentiality by an employee, the employee will be terminated.

## CONFIDENTIALITY AGREEMENT

I understand that in the performance of my duties I will come in contact with confidential information and that it is part of my job to protect this information. I understand that confidential information comes in many forms and from many sources. For example, it can be generated from the medical, computer operations, logs, personnel files, etc. I further understand that the aforementioned sources may only be accessed and discussed if the information is required to perform my job duties. I also realize that it is my responsibility to report to the Practice Administrator any breach of confidentiality that I witness.

By signing below, I confirm that I have received a copy of the clinic's confidentiality and release of information policies and will uphold their contents. I understand that my continued employment/assignment at the clinic may be contingent upon my compliance with these policies and that violations of these policies may result in disciplinary action, up to and including termination.

Witness Date

Employee Date

**Authorized Signature**

# Authorization to Use and Disclose Protected Health Information

**Authorization to release the protected health information of:**

| Patient Name: | MRN (office use Only): | EMPI#(office use Only): |
|---|---|---|

Current Address | City | State | Zip

Phone Number ( ) | Date of Birth / /

**This authorization is to release the protected health information to:**

Name | Phone Number ( )

Address | City | State | Zip

Deliver by: ☐ In Person ☐ Mail ☐ By Phone ☐ Fax Fax Number :
☐ Secure Email Secure Email Address:
☐ Secure Audio/Video Connection:

**This authorization is to release the protected health information from:**

Facility Name/Provider | Phone Number ( )

**The purpose of this disclosure is:**

**Dates of service requested:**

**Release the following information:**

***Patient Health Information:***

| | | |
|---|---|---|
| ☐ Discharge Summary | ☐ Pathology report(s) | ☐ Behavioral Health Admitting Evaluation |
| ☐ History & Physical | ☐ Radiology report(s) | ☐ Behavioral Health Discharge Summary |
| ☐ Consultation(s) | ☐ Lab report(s) | ☐ Mental Health Therapy Records |
| ☐ Operative report(s) | ☐ Cardiology report(s) | ☐ Other records as specified |
| ☐ Progress notes | ☐ Treatment Plan(s) | ☐ Emergency record(s) |

☐ Substance Use Disorder Treatment Record(s)_____

***Financial:***

☐ Itemized Billing Statement ☐ Financial Information

**This Authorization will remain in effect:**

☐ From the date of this Authorization or until the following event occurs:_____

Unless otherwise noted above this authorization will remain in effect 180 days from the date signed

I understand that:

- Once *"this facility"* discloses my health information by my request, it cannot guarantee that the Recipient will not re-disclose my health information to a third party. The third party may not be required to abide by this Authorization or applicable federal and state law governing the use and disclosure of my health information.
- I may make a request in writing at any time to *"this facility"* to inspect and/or obtain a copy of my health information maintained at this facility as provided in the Federal Privacy Rule 45 CFR § 164.524.
- This Authorization will remain in effect until the Authorization expires or I provide a written notice of revocation to the Health Information Management/Medical Record Department. If I revoke this Authorization, Intermountain Healthcare may not be able to reverse the use of disclosure of my health information while the Authorization was in effect.
- I may refuse to sign or may revoke this Authorization at any time for any reason and that such refusal or revocation will not affect the commencement, continuation or quality of *"this facility"* treatment of me, enrollment in the health plan, or eligibility for benefits.
- Substance Use Disorder treatment records are protected by Federal Rule 42 CFR, part 2. Both a minor's and a parent guardian's signature must be obtained prior to disclosing the minor's Substance Abuse Disorder records.
- If I have questions about disclosure of my health information, I can contact the facility / clinic Medical Record Department, or call 844-442-1987.
- 我們將根據您的需求提供免費的口譯服務。請找尋工作人員協助;
- Si lo solicita, se le proveerá un servicio de interpretación gratis. Hable con un empleado del hospital para solicitarlo.
- If requested, we will provide you a free interpretation service. Talk to an employee of the hospital to apply.

| Signature of Patient or Personal Representative: | Date |
|---|---|
| If Signed by Personal Representative, Relationship: | Signature of Witness (optional) |

Original (Medical Record) Copy (Patient)

*503

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | De-Identification of PHI | | | Policy # | 708 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 2 | |
| Policy Section | HIPAA Policies | | | | |

**PURPOSE:**

To assure compliance that supports HIPAA regulations.

**POLICY:**

It is the policy of Ponderosa Family Care to secure and maintain the medical records of each and every patient receiving clinic services.

**PROCEDURE:**

1. The clinic has a duty to protect the confidentiality and integrity of PHI as required by law, professional ethics, and accreditation requirements. Whenever possible, de-identified PHI should be used. De-identified PHI is rendered anonymous when identifying characteristics are completely removed. PHI must be de-identified prior to disclosure to non-authorized users. This policy defines the guidelines and procedures that must be followed for the de-identification of PHI.

2. All personnel must strictly observe the following standards relating to the de-identification of PHI:
   A. De-identification requires the elimination not only of primary or obvious identifiers, such as the patient's name, address, date of birth (DOB), and treating physician, but also of secondary identifiers through which a user could deduce the patient's identity. For information to be de-identified the following identifiers of the individual (or of relatives, employers, or household member of the individual) must be removed:
      i. Names
      ii. Address information smaller than a state, including street address, city, county, zip code (except if by combining all zip codes with the same initial three digits, there are more than 20,000 people)
      iii. Names of relatives and employers
      iv. All element of dates (except year), including DOB, admission date, discharge date, date of death; and all ages over 89 and all elements of dates including year indicative of such age except that such ages and elements may be aggregated into a single category of age 90 or older:
         a) Telephone numbers
         b) Fax numbers
         c) Email addresses
         d) Social Security Number (SSN)

e) Medical Record Number
f) Health beneficiary plan number
g) Account numbers
h) Certificate/License Number
i) Vehicle identifiers, including license plate numbers
j) Device ID and serial number
k) Uniform Resource Locator (URL)
l) Identifier Protocol (IP) addresses
m) Biometric identifiers
n) Full face photographic images and other comparable images
o) Any other unique identifying number characteristic, or code

v. Whenever possible, de-identified PHI should be used for quality assurance monitoring and routine utilization reporting. If de-identified PHI cannot be used, a limited data set should be used whenever possible.

vi. PHI used for research, including public health research, should be de-identified at the point of data collection for research protocols approved by the clinic, unless the participant voluntarily and expressly consents to the use of his/her personally identifiable information or a clinic waiver of authorization is obtained. If de-identified PHI cannot be used for research, a limited data set should be used whenever possible.

vii. If an authorized user wishes to encrypt PHI when creating de-identified information the authorized user must ensure that:
   a) The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual.
   b) Anyone involved in the research project does not use or disclose the code or other means or record identification and does not disclose the mechanism to accomplish re-identification.

viii. If removal of any identifiers is not practical or does not meet your business needs and you still wish to use PHI, you must obtain approval from the Practice Administrator.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Designated Record Set | | | Policy # | 709 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 3 | |
| Policy Section | HIPAA Policies | | | | |

**PURPOSE:**

HIPAA regulations state that patients have a right to access portions of their medical record, which is called the Designated Record set. The purpose of this policy is to define what is included in the HIPAA-compliant Designated Record Set that is subject to access by individuals (patients) for purposes of obtaining copies of or amending their PHI.

**POLICY:**

Designated Record Set definition for Ponderosa Family Care is defined with a multi-layered strategy to facilitate management of the processes surrounding patient inspection, copying, restriction and amendment of the records that fit the definition.

**PROCEDURE:**

Ponderosa Family Care will engage all individuals making proper HIPAA requests (i.e. requests for access, amendment, disclosure accounting, restriction, or confidential communications) to fully understand and communicate the plans to fulfill these requests in a manner that satisfies the individual and keeps the administrative burden manageable for Ponderosa Family Care.

PRIVACY RULE DEFINITION OF A DESIGNATED RECORD SET

The Privacy Rule (section 164.501) provides the following definitions for Designated Record Set and PHI in order to clarify the access and amendment standards summarized in the previous paragraphs.

Designated Record Set is defined as a group of records maintained by or for a CE that is:

1. The medical and billing records about individuals maintained by or for a covered healthcare provider. These records are the primary source of Designated Record Set records for Ponderosa Family Care by patients for copying, inspection and amendment and include medical records and Business Office documents and reports. These records are generally more accessible, understandable by patients and include complete summaries and reflections of the complete documentation for patient care and billing. Other Ponderosa Family Care source systems may not be designed to easily facilitate these tasks, and again, are redundant to the information kept within the primary medical records and Business Office records.

2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan if a part of Ponderosa Family Care.

3. Information used in whole or in part by or for the CE to make decisions about individuals. The record, data, document and report sets may occur in a multitude of other Ponderosa Family Care 'Source Systems' and would be subject to patient inspection, copying and amendment only upon determination that such inspection, copying, and amendment is necessary to archive the patient's goals, is deemed appropriate given the restrictions to these activities that HIPAA defines (see below for further explanation for these exceptions) and is technically possible.

4. According to the preamble of the Privacy Rule, records held by a Business Associate that meet the definition of Designated Record Set are part of the CE's Designated Record Set. However, the individual's rights to access, amend, and receive an accounting of disclosures does not attach to the BA's records if the BA's information is the same as the information maintained by the CE.

5. Uses or disclosures that are required by Law; and

6. To meet the requirements of HIPAA, such as for the content of standard transactions.

RECORD SETS NOT INCLUDED IN THE DESIGNATED RECORD SET

The preamble of the Privacy Rule emphasizes that individuals have a right to access and request amendments only to PHI in a Designated Record Set. Therefore, information obtained during a phone conversation, for example, is subject to access only to the extent that it is recorded in the Designated Record Set. The Rule does not require a CE to provide access to all individually identifiable health information, because the benefits of access to information not used to make decision about individuals is limited and is outweighed by the burdens of locating, retrieving, and providing access to such information.

The preamble also underscores the fact that CEs often incorporate the same PHI in a variety of different data systems, not all of which will be used to make decisions about individuals. The preamble provides an example in which information systems used for quality control or peer review analysis may not be used to make decisions about individuals. In this example, the preamble says the information systems would not fall within the definition of Designated Record Set. Furthermore, the preamble states that it does not require entities to grant an individual access to PHI maintained in these types of information systems.

THE PRIVACY RULE AND DISCUSSION IN THE PREAMBLE ALSO MAKE IT CLEAR THAT INDIVIDUALS DO NOT HAVE A RIGHT OF ACCESS TO:

1. Psychotherapy notes

2. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

3. PHI held by clinical laboratories if the Clinical Laboratory Improvements Amendments of 1988 (CLIA) prohibit such access

4. PHI held by certain research laboratories that are exempt from the CLIA regulations (164.524).

The Rule defines, however, rare circumstances in which access to information contained within the Designated Record Set can be denied. For example, access can be denied when, in the exercise of professional judgment, it is likely to endanger the life or physical safety of the individual or another person.

ADDITIONAL, SPECIFIC INFORMATION NOT INCLUDED IN THE Ponderosa Family Care DESIGNATED RECORD SET

1. Health information generated, collected, or maintained for purposes that do not include decision making about the patient or which is exempt from disclosure to the patient:
   A. Data collected and maintained for research.
   B. Data collected and maintained for peer review purposes.
   C. Data collected and maintained for performance improvement purposes.
   D. Data collected and maintained for quality control purposes.
   E. Data collected and maintained for compliance purposes.
   F. Data collected and maintained by the psychiatric Patient's Rights Officer.
   G. Appointment and surgery schedules.
   H. Birth and death registers.
   I. Surgery registers.
   J. Diagnostic or operative indexes.

2. Information compiled in reasonable anticipation of or fur use in a civil, criminal, or administrative action or proceeding. This includes notes taken by the Ponderosa Family Care employees during a meeting with Ponderosa Family Care's attorney about a pending lawsuit.

3. Employer records
   A. All employee health records.

4. Source Data—interpreted or summarized in the individual's medical record
   A. Pathology slides
   B. Diagnostic films
   C. Electrocardiogram tracings from which interpretations are derived
   D. Photographs
   E. Fetal Monitor Strips
   F. Clinic EHR system's name data, documents and reports.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Device and Media Control | | | Policy # | 710 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 2 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

To define guidelines for managing digital devices with the intent to prevent Protected Health Information (PHI) breach and/or HIPAA violations arising from PHI storage on the hard disk drives or memory of these digital devices.

## POLICY:

Ponderosa Family Care has adopted this policy to ensure that PHI is not wrongfully disclosed by way of stored images or data memory within digital copiers, printers, scanners, medical devices, and fax machines.

Since 2002, most digital printers, photocopiers, scanners and fax machines have been manufactured to operate with an internal hard drive or memory that captures images of every document processed. Safeguards to protect information on these devices must be followed to prevent possible HIPAA violations and/or breeches caused by theft, unauthorized access, use, or disclosure; improper modification or destruction data.

As a general rule, Ponderosa Family Care requires ALL copier, scanner and medical device companies to sign Business Associate Agreements and acknowledge that their technicians are trained on secure management of PHI.

## PROCEDURE:

Information security policies and safeguards for protecting data stored on digital copiers and other devices may include the use of automated software routines that wipe clean any stored images on a routine basis. Other mechanisms for securing data may include the use of pass codes or encryption of all images on these disks. Encryption guidelines should be utilized to create secured PHI or destruction of stored images by technicians on scheduled or on-demand basis.

PROCEDURE FOR NEW EQUIPMENT PROCUREMENT

1. When buying or leasing new equipment, investigate and evaluate manufacture options for securing data on digital devices. Ensure that sales representatives selling/leasing the equipment are aware of the Ponderosa Family Care security concerns and requirements.

2. Procurement software or other mechanisms that, ideally, destroy or encrypt according to NIST 800-66 guidelines (creating secured PHI) stored images immediately after each use or on a set basis, such as daily.

3. Set-up routine maintenance procedures to investigate whether or not this image destruction is occurring.

FOR EXISTING EQUIPMENT (ALREADY PURCHASED)

1. Investigate with the vendor of the product the status of stored images and hard drives within each copier, scanner and medical device.

2. Determine if auto destruction or encryption routines are available for each unit and institute if possible.

3. Ensure that routine and on demand maintenance visits by technicians address this issue.

4. Never allow any equipment that may have hard drives to leave the premises without ensuring that all stored images have been destroyed or encrypted.

EQUIPMENT THAT IS TO BE SOLD, TRADED OR DISPOSED OF

1. Determine the hard drive and stored image status of any machines to be sold, traded or disposed of BEFORE they leave the Ponderosa Family Care property.

2. Ensure any hard drives are completely scrubbed clean (preferably according to NIST 800-66 destruction guidelines) prior to leaving the Ponderosa Family Care property.

3. Hard drives may be crushed or rendered unusable through certified destruction as an alternative to scrubbing.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Disposal of Patient Information | | | Policy # | 711 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 1 | |
| Policy Section | HIPAA Policies | | | | |

**PURPOSE:**

To assure compliance that supports HIPAA regulations.

**POLICY:**

It is the policy of Ponderosa Family Care to secure and maintain the medical records of each and every patient receiving clinic services.

**PROCEDURE:**

1. PHI must not be discarded in trash bins, unsecured recycle bags or other publicly accessible locations. Information must be shredded or placed in a secured recycling bag.

2. Printed material and electronic data containing PHI shall be disposed of in a manner that ensures confidentiality.

3. It is the individual's responsibility to ensure that the document has been secured or destroyed. It is the Practice Administrator responsibility to ensure that employees are adhering to the policy.

4. The Practice Administrator shall provide employees with access to shredders or secured recycling bags for proper disposal of confidential printouts containing PHI.

5. The employee may elect to use either shredding or secure recycle bags for the destruction of convenience copies, as long as the destruction is in accordance with this policy.

6. Secure methods will be used to dispose of electronic data and output. The Practice Administrator is responsible for the destruction of electronic copies containing PHI. However, employees may dispose of the electronic data themselves using the following methods:
   A. Deleting on-line data using the appropriate utilities.
   B. "Degaussing" (removing or neutralizing the magnetic field) computer tapes to prevent recovery of data.
   C. Erasing diskettes to be re-used using a special utility to prevent recovery of data.
   D. Destroying discarded diskettes.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Documentation Authentication Signature | | | Policy # | 712 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 1 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

The health care provider who treats a patient shall have the responsibility for documenting and authenticating the care rendered. Such documentation shall be in accordance with documentation guidelines developed in concert with this policy statement and approved by the advisory committee.

## POLICY:

It is the policy of Ponderosa Family Care to secure and maintain the medical records of each and every patient receiving clinic services.

## PROCEDURE:

Proper authentication shall be added at the conclusion of each entry and shall consist of the midlevel provider signature. The staff member's first name, full last name and credentials shall be added at the conclusion of each entry they document.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Documentation for Security & Privacy Compliance | | | Policy # | 713 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 2 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

The purpose of this policy is to provide guidance on development, management and maintenance of documentation related to HIPAA requests, complaints, investigations and ongoing compliance activities.

## POLICY:

This policy is intended to govern the creation, use, and maintenance of documentation (documents) related to HIPAA compliance. Workforce members must document in writing (or in electronic format) all HIPAA related activities that require documentation. Any action, activity or assessment that must be documented shall be stored or maintained in accordance with this and other policies and procedures implemented by Ponderosa Family Care. Such documentation must be used, applied and reported according to the law and other Ponderosa Family Care policies.

Ponderosa Family Care retains all HIPAA-related documentation for a minimum of six (6) years from the date of its creation or modification, or the date when it was last in effect, whichever is later. All workforce members need to have appropriate access to security and privacy policies and procedures, which should be organized in a logical, indexed fashion for ease of retrieval. Policies and procedures addressing documentation of Security and Privacy compliance must be regularly updated and maintained for accuracy. Changes introduced by technology (especially those impacting investigation, logging and tracking or documenting and reporting on security or privacy events/incidents, requests, complaints, etc) should be reflected and addressed in the Ponderosa Family Care's compliance program documents.

Technology is increasingly required to manage complex security and privacy compliance programs. As new technologies are introduced, the Ponderosa Family Care's policies and procedures should be updated any time there is a material change to the processes or safeguards that the technology introduces.

Documentation to be strongly considered for retention throughout the entire HIPAA-defined retention period includes, but is not limited to the following list:

*Appropriate workforce members who need access to this information must be provided such access.*

1. Security Risk Assessment (Analysis), also known as (SRA)

2. Privacy Risk Assessment (PRA)

3. Privacy and Security Risk Management Plan and all program-related documentation
4. Sanction and mitigation activities
5. Business Associate Agreements (or if a BA, Sub-contractor Agreements), Confidentiality Agreements and other privacy or security compliance agreements or contracts
6. Wrongful disclosure violation/breach detection, investigation, determination and notification forms.
7. Configuration, update and patch management
8. Results of disaster recovery test plans, results, emergency testing and business continuity documentation
9. List of software used to manage and control internet access and use
10. Penetration testing and vulnerability scans
11. Security issues logs
12. List of workstations, their use and employees who can access them
13. Audit log copies
14. Business Associates and other agreement documentation surrounding the protections of privacy and security in congruence with the Ponderosa Family Care policies
15. Business Associate ongoing compliance monitoring
16. Documentation surrounding Patient Rights requests (Individual Access to PHI, Amendment, Restrictions, Account of Disclosure forms), any Confidential Communications, etc.
17. Proactive, concurrent and retrospective access; other privacy audits and reviews
18. Privacy and security education and training
19. Other general security and privacy documentation

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Email Policy | | | Policy # | 714 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 7 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

The Ponderosa Family Care's electronic mail has become an integrated tool in Organization business processes. This policy defines the requirements for email usage at the Organization. Electronic mail is designed to facilitate business communications and is not to be used in a way that may be disruptive, offensive to others or harmful to morale. Particular care must be given restricting the amount of PHI contained in any emails to the HIPAA Minimum Necessary and all emails containing PHI must be secured. This policy and all related procedures define the minimum requirements for Organization email usage and are applicable to all Organization workforce members.

## POLICY:

### Procedures

### General Use – Email

Organization email systems shall be used primarily for business use. Personal use of Organization email systems shall be limited to a level that does not impede worker productivity. The content of all emails shall be used in a way that does not disrupt or offend others, harm morale or create security exposures. Members of the Organization workforce shall ensure that the business information contained in email messages is accurate, appropriate and lawful. When sending email attachment files, caution shall be taken by members of Organization's workforce that the correct file is being attached. Recipient's authentication shall be performed (by the sender) prior to the transmission of all Organization emails to ensure that the content is only accessible by the intended recipient.

### User Responsibilities

The user is any person who has been authorized to read, enter, or update information created or transmitted via Organization electronic mail system. Electronic mail is to be used as a business tool to facilitate communications and the exchange of information needed to perform an employee's job. Incidental personal use is permissible so long as: (a) it does not consume more than a trivial amount of resources, (b) does not interfere with worker productivity, and (c) does not preempt any business activity.

Users have an obligation to use email appropriately, effectively, and efficiently. Users must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed and stored by others. Therefore, users must utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents.

Organization email accounts and passwords should not be shared or revealed to anyone else besides the authorized user(s).

**Right to Monitor Email and Communications**

Management reserves the right to audit an employee's email and communication system files (including email files). Messages generated within and/or transmitted through Organization email and/or communication systems are to be considered neither private nor confidential. Organization reserves the right to intercept, monitor, access, and/or disclose any information that is maintained on, stored in or transmitted through its email or communication systems for any purpose. Upon separation of service, members of the Organization workforce shall not retain any rights to contents of the Organization email and/or communications systems. Additionally, all messages distributed via Organization email and communication systems (including through non- Organization email addresses) are subject to monitoring by Information Technology (IT), and disclosure to law enforcement or government officials or to other third parties through subpoena or other processes.

Electronic mail information is occasionally visible to IT staff engaged in routine testing, maintenance, and problem resolution. Staff assigned to carry out such assignments will not intentionally seek out and read, or disclose to others, the content of email.

Management must advise and receive approval from the Human Resources Department, in conjunction with the HIPAA Security Officer, as appropriate, of their intent to review an employee's messages prior to accessing employee files.

**Prohibited Uses**

Certain activities are prohibited with regard to use of Organization email and communication systems. The list below provides a framework for activities that fall into the category of unacceptable use. This list is not exhaustive and Organization has the right to decide any activity is inappropriate at its discretion:

1. Using Organization email and communication systems for effecting security breaches or disruptions of network communication.

2. Engaging in any activity that is illegal under local, state, federal or international law while utilizing any Organization IT system or data.

3. Copying or transmission of any document, software or other information protected by copyright and/or patent law, without proper authorization by the copyright or patent owner;

4. Engaging in any communication that is threatening, defamatory, obscene, offensive, or harassing.

5. Use of email system for unauthorized solicitation of funds, political messages, gambling, commercial, or illegal activities.

6. Disclosure of an individual's personal information or a patient's protected health information (PHI) without appropriate authorization.

7. Transmission of information to individuals inside or outside the Organization without a legitimate business need for the information.

8. Use of email addresses for marketing purposes without explicit authorization from the target recipient.

9. Forwarding of email from in-house or outside legal counsel, or the contents of that mail, to individuals outside of the Organization without the express authorization of counsel.

10. Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communication.

11. Obtaining access to the files or communications of others with no substantial organization business purpose and beyond the individual's "need to know".

12. Attempting unauthorized access to data or attempting to breach any security measure on any electronic communication system, or attempting to intercept any electronic communication transmissions without proper authorization.

13. Sending external transmission of confidential information via Organization email and communication systems, including email attachments without proper authorization, authentication and encryption.

14. Excessive personal use and/or unethical use of Organization's email and communication systems.

15. Using Organization's electronic mail and other information systems, such as communication, in a way that may be disruptive, offensive to others or harmful to morale.

16. Opening, responding to, or forwarding email messages from any unknown source.

17. Displaying or transmitting sexually explicit images, messages, games, cartoons or anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, marital status, veteran status, age, disability or religious or political beliefs. Email is subject to the Organization policy and procedures governing sexual harassment and discrimination. Sending or forwarding offensive material violates this policy as well as the business use policy.

18. Using Organization email and communication systems to solicit others for commercial ventures, religious or political causes, outside organizations not approved of by Organization, or in any other non-job-related situations.

19. Circumventing user authentication or physical security controls to access Organization email and communication systems.

20. Copying, transmitting or providing information about Organization email and communication systems to any individual without proper authorization.

This list is not considered all-inclusive or collectively exhaustive. Further questions regarding appropriate use of electronic mail should be directed to the employee's supervisor or Organization HIPAA Security Officer.

**Confidentiality of Electronic Mail**

Users of Organization electronic mail system may have the capacity to forward, print and circulate any message transmitted through the system. Therefore, users are to utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents. When email is used for communication of confidential or sensitive information, specific measures must be taken to safeguard the confidentiality of the information.

These safeguards are as follows:

1. Information considered confidential or sensitive should be protected during storage of the data utilizing encryption or password protection that ensure the information is not accessed by anyone other than the intended recipient.

2. Any PHI transmitted must be the Minimum Necessary amount, as defined by HIPAA Policy.

3. Confidential or sensitive information may be distributed to multiple recipients.

4. Confidential or sensitive information is to be distributed only to those with a legitimate need to know.

The following internally generated notation is to be included on all email messages, including external email messages:

Confidentiality Notice: This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

Please be aware that email communication can be intercepted in transmission or misdirected. Your use of email to communicate protected health information to us indicates that you acknowledge and

accept the possible risks associated with such communication. Please consider communicating any sensitive information by telephone, fax or mail. If you do not wish to have your information sent by email, please contact the sender immediately.

**Retention of Electronic Mail**

Generally, email messages constitute temporary communications, which are non-vital and may be discarded routinely. However, depending on the content of an email message, it may be considered a more formal record and should be retained pursuant to organization record retention schedules.

Email will not be routinely made a part of any client's medical records by Organization. Email will be included in medical records only if there is a note otherwise documented in the medical record indicating that this copy is necessary and there is a direct relationship to care rendered during the encounter for which the medical record is serving as the business record documenting that care. The clinician recording the note about the email is responsible for making sure a copy of the email is placed into the medical record.

Electronic mail that users wish to or are required to retain must be moved to a permanent folder on their workstation.

Electronic mail tape back-ups are performed on a regular basis for the purpose of business recovery. Electronic mail data that could be used or relevant to an OCR investigation is retained for 6 years.

**Organization Electronic Mail of Protected Health Information (PHI)**

Emailing confidential patient information necessary for the performance of your job is specifically authorized within the Organization network if minimally necessary information is sent. Any email communication of confidential patient information (protected health information) to non Organization personnel or Organization personnel outside the Organization network is specifically disallowed, except under the following conditions:

1. The request for this type of release has been forwarded to the Practice Administrator for review and processing.

2. The Patient/Designated Representative has signed a valid authorization specifically allowing such communication, and has been informed of all potential security risks and that this mode of transmission may not be secure. Organization staff will document such authorizations in the clinical record.

3. Verbal authorizations will be documented and witnessed on an authorization form by office manger, but are not considered an optimal method to communicate an authorization. If it is impractical to forward to Practice Administrator the request and rather than a verbal authorization, the e-mail authorization procedure listed below should be used.

4. The communication to an authorized recipient is accomplished in a way that it would be impossible to determine the identity of the patient if it were illegitimately intercepted.

5. The Patient/Designated Representative must be informed that the authorization to release may be revoked at any time in writing, except to the extent it has been acted upon. The authorization will be effective only long enough to answer the purpose for which it is given, and no further confidential information will be released without the execution of an additional authorization.

Note: Certain protected health information (PHI) require special consents, e.g. PHI related to HIV, genetic testing, venereal disease, psychotherapy notes, drug/alcohol. Emailing confidential information of this type is specifically prohibited by the organization workforce.

All misdirected email containing PHI must be documented and reported in accordance with the Information Security-Breach Notification Policy.

**Email Authorization Procedure**

This procedure is recommended as opposed to verbal authorizations to communicate PHI and patient information by email only if Practice Administrator reviews are not practical for a given circumstance.

Organization may obtain informed consent from a patient or designated representative through email by conducting the following consent exchange upon presentation of a patient query (this example is for an email exchange):

I will be happy to respond to your query but to do so by email you must provide your consent, recognizing that email is not a secure form of communication. There is some risk that any protected health information that may be contained in such email may be disclosed to, or intercepted by unauthorized third parties. I will use the minimum necessary amount of protected health information to respond to your query.

If you wish to conduct this discussion by email, please indicate your acceptance of this risk with your email reply. Alternatively, please call my office to arrange a phone conversation or office visit.

Note: Extra care should be taken by the sender to assure that the sender is confident of the correspondent's identity, that any PHI be kept to a minimum and that, as with phone or fax based exchanges, this consultation be documented in the patient's record if appropriate. Further, even when requested by a patient, the provider should decline to use email and refer to phone or office visit if she or he has any concerns about any aspect of the exchange.

**Responsibilities:**

Organization MANAGEMENT

Organization Management shall ensure their staff adheres to the requirements outlined in this policy and all subordinate procedures related to email and communication systems. Management must immediately report any known or suspected breach of security policy to the HIPAA Security Officer.

Organization WORKFORCE

All workforce members shall comply with this policy and all referenced policies to ensure privacy of sensitive information. Members of the Organization workforce shall report any known or suspected breach of this policy and/or its subordinate procedures to management or the HIPAA Security Officer.

Organization BUSINESS ASSOCIATES

All business associates of organization shall comply with this policy to ensure the privacy and security of protected health information (PHI). Any known breach, shall be immediately reported to the HIPAA Security Officer.

Organization INFORMATION TECHNOLOGY (IT)

Organization Information Technology (IT) shall maintain and update all policies related to email and communication system usage to ensure that they are comprehensive and consistent with local, state, federal and international law. IT shall ensure that all responsibilities for carrying out the requirements outlined within this policy are delegated to qualified staff. IT reserves the right to intercept, monitor, access, and/or disclose any information that is maintained on, stored in or transmitted through its email or communication systems for any purpose. The HIPAA Security Officer shall be made aware of any breach of security policy and advise Human Resources as to the severity of the breach.

**Accountability**

All Organization workforce members with access to Organization information systems who are found to be in violation of any part of this policy are subject to disciplinary action, up to and including termination of employment or contract and legal action. IT will immediately suspend email system access privileges to any authorized user when unacceptable use severely impacts system performance or security. Retaliatory action shall not be taken against individuals who identify and/or report violations of security policy.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Fax Transmittal of PHI | | | Policy # | 715 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 2 | |
| Policy Section | HIPAA Policies | | | | |

**PURPOSE:**

To assure compliance that supports HIPAA regulations.

**POLICY:**

It is the policy of Ponderosa Family Care to secure and maintain the medical records of each and every patient receiving clinic services.

**PROCEDURE:**

1. The clinic protects the facsimile transmittal of PHI and holds individuals responsible for following the proper procedure when PHI is sent via facsimile. The clinic protects the confidentiality and integrity of confidential medical information as required by law and professional ethics.

2. PHI will be sent by facsimile only when the original record or mail delivered copies will not meet the needs for TPO. For example, personnel may transmit PHI by facsimile when urgently needed for patient care or required by a third party payer for ongoing certification of payment for a patient.

3. Information transmitted must be limited to the minimum necessary to meet the requester's needs.

4. Except as authorized by the individual's consent to TPO or federal or state law, a properly completed and signed authorization must be obtained before releasing PHI. The following types of medical information are protected by federal and/or state statute and may NOT be faxed or photocopied without specific written patient authorization, unless required by law:
   A. Psychotherapy records of treatment by a psychiatrist, licensed psychologist or psychiatric clinical nurse specialist.
   B. Other professional services of a licensed psychologist.
   C. social work counseling/therapy.
   D. Domestic violence victim's counseling.
   E. Sexual assault counseling.
   F. Records pertaining to sexually-transmitted diseases.
   G. HIV test results.
   H. Alcohol and drug abuse records.

5. The Facsimile Cover Letter must be used to send faxes containing PHI. All pages plus the cover page of all confidential documents to be faxed must be marked "Confidential" before they are transmitted.
6. Personnel must make reasonable efforts to ensure that they send the facsimile transmission to the correct destination including:
   A. Preprogramming frequently used numbers into the machine to prevent misdialing errors.
   B. Periodically and/or randomly checking all speed-dial numbers to ensure their currency, validity, accuracy, and authorization to receive confidential information.
   C. For a new recipient, the sender must verify the fax number by requesting the recipient submit a faxed or e-mail request for PHI, which would include the fax number of the recipient.
   D. Periodically reminding those who are frequent recipients of PHI to notify the clinic if their fax number is to change.

7. For TPO purposes, it is not required to maintain a copy of the fax transmittal or fax confirmation sheet. For Non-TPO purposes and without a signed authorization from the patient an accounting of the disclosure must be maintained.

8. If a fax transmission-containing PHI is not received by the intended recipient because of a misdial, check the internal logging system of the fax machine to obtain the misdialed number.

9. If possible, a phone call (supplemented by a note referencing the conversation) should be made to the recipient of the misdirected fax requesting that the entire content of the misdirected fax be destroyed. If the recipient cannot be reached by phone, a fax using the Letter for Misdirected Fax should be sent to the recipient requesting that the entire content of the misdirected fax be destroyed.

10. Misdirected faxes will be recorded on the patient's Accounting of Disclosure form.

11. Fax machines used for patient care or patient related services shall not be located in areas accessible to the general public but rather must be in secure areas.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Handling Privacy Complaints/Internal & External | | | Policy # | 716 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 4 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

To support the Organization as we continually improve the quality of services provided and to define a process for handling complaints and grievances related to the use or disclosure of Protected Health Information (PHI).

## POLICY:

1. HIPAA privacy and security laws and rules grant individuals (patients) specific 'rights' relating to their PHI, many of which overlap with patient rights mandated by state law. In addition to privacy rights related to their PHI, individuals (patients) are granted the right to: access their PHI/medical record information; request restrictions on the use or disclosure of their PHI; request that communications related to their PHI be confidential; request an amendment to their PHI; and receive an Accounting of Disclosures of their PHI. HIPAA also mandates that a Covered Entity (CE) implement a process for individuals to submit a complaint about the CE's privacy-related policies and procedures and its compliance with those policies and procedures.

2. Complaints may be related to privacy and/or security issues. This policy is focused more on privacy complaints; however, determinations in the nature of any privacy/security complaint and the resulting, appropriate mitigations and/or sanctions will be applied equally and by the responsible privacy or security compliance parties within this Organization.

3. Privacy complaints (which may be in the form of a grievance) about wrongful access, use or disclosure of PHI, or for any other HIPAA or State regulatory based reason, may come from external sources such as patients themselves, the State or Federal regulators (Office for Civil Rights (OCR), typically), from an internal channel or workforce member.

4. All privacy complaints, regardless of the source, about HIPAA 'rights', access, use or disclosure of PHI shall be investigated and managed in a timely and respectful manner.

5. Complaints concerning PHI, their investigation, disposition or resolution must be documented in writing (or within a computer system) and shall be kept for the appropriate retention period(s) prescribed by regulation.

6. To the extent practicable, any known harmful effect of an access, use or disclosure of PHI in violation of our policies and procedures and the requirements of applicable laws, by any Covered Entity or Business Associate must be mitigated.

7. Our Organization will not retaliate in any way (i.e. intimidation, threatening behavior, coercion, and discrimination) against an individual lodging a complaint, or for testifying, assisting, or participating in any investigation or administrative action. Nor will any individual be asked to waive the rights permitted to him or her under State or Federal Privacy Laws as a condition of treatment, payment, enrollment, or eligibility for benefits.

**Responsible Parties**

The Privacy Officer is responsible for overseeing the management and documentation requirements related to privacy complaints regarding HIPAA rights, access, use or disclosure of PHI. The Security Officer manages security based complaints and works together with the Privacy Officer to form a unified Privacy and Security Compliance Program.

**Procedure**

Respond to complaint in writing.

1. Consider confidentiality concerns (i.e., if a relative informed you of the concerns, do you have the authority to discuss the patient health care information with the relative, or do you need a signed consent form?).

2. Notify or consult with the appropriate Organization insurance carrier and/or legal counsel on issues involving liability and litigation potential.

3. Respond in a timely fashion (i.e., the initial response could simply be that the Organization will investigate and inform you of the final decision if enough information is not available to make an immediate determination). A letter with the final resolution or disposition shall be sent to the appropriate party, the individual or the regulatory body.

4. Notify the appropriate individual to address any pertinent employment issues (i.e. investigation, counseling, disciplinary action, or termination) according to applicable policies/procedures and State and Federal Laws.

5. Work to mitigate, to the extent practicable, any harmful effect that is known because of an access, use or disclosure of PHI in violation of organizational policies and procedures or the requirements of applicable laws by the Organization or their Business Associates.

6. Take steps to ensure that the Organization will not retaliate in any way (i.e., intimidation, threatening behavior, coercion, and discrimination) against an individual lodging a complaint or grievance.

7. If the results of the investigation indicate that an employee or Business Associate of the Organization made an unauthorized access, use or disclosure relating to a patient's rights in regards to PHI; failed to maintain the privacy of the patient's PHI; failed to request restrictions on uses or disclosures of the patient's PHI, or otherwise violated the practice's HIPAA policies

and procedures it should be reported to the Privacy Officer. If the investigation was conducted by the Privacy Officer, the Privacy Officer shall report it to the practice's governing body.

8. Follow-up, mitigate and provide sanctions as appropriate.

9. The Privacy Officer shall document all HIPAA-related complaints, their resolution, and any actions resulting therefore. This documentation must be maintained for a minimum period of six (6) years from the date of final resolution, unless modified by State or Federal regulation and defined within another policy.

**Tips for Workforce Members Responding to a Privacy Complaint**

1. Listen – communication considerations:
   A. Actively listen. Take steps to minimize interruptions by others and interrupting the individual.
   B. Restate your understanding of the nature of the issue.

2. Address the individual's concern if authorized and able to do so, or advise the individual that you would be happy to report the problem or that he or she may report the problem to your immediate Supervisor. Consider the following:
   A. Again, remember confidentiality concerns (i.e., if a relative informed you of the concerns, do you have the authority to discuss the patient health care information with the relative, or do you need a signed consent form?).
   B. An individual has the right to request to file a written complaint with the Privacy Officer.
   C. If the individual expresses a desire to complain to the Department of Health and Human Services or the Office for Civil Rights (OCR), advise the individual that "we also respect your right to file a complaint with the OCR and that the Organization will not retaliate against you." OCR complaints should be filed online at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html

3. Document in writing all discussions and maintain notes and any information useful for an investigation. This document should be routed immediately to the Privacy Officer.

**Definitions**

**Complaint (or Grievance)**

Any concern communicated verbally or in writing by a patient (or a patient's legal representative) questioning any act or failure to act by our Organization relating to a patient's rights to access the patient's protected health information; to maintain the privacy of the patient's protected health information; to request restrictions on uses or disclosures of the patient's protected health information, to request confidential communications regarding the patient's protected health information (PHI); to request an amendment to the patient's protected health information, or to receive an accounting of disclosures of the patient's protected health information.

**Protected Health Information (PHI)**

Individually identifiable health information relating to the past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care services provided to an individual. ePHI refers to electronically (computerized) created or stored protected health information.

**Responsible Party**

The Privacy Officer is responsible for overseeing the management and documentation requirements related to complaints regarding the use or disclosure of PHI. This individual also reviews and responds to complaints concerning PHI as needed.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Individual Access to PHI | | | Policy # | 717 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 6 | |
| Policy Section | HIPAA Policies | | | | |

**PURPOSE:**

Specifics on how individuals (patients or their authorized representatives) may request access and copies of their Protected Health Information contained within designated records sets.

**POLICY:**

Individuals (patients or their authorized representatives) who wish to access PHI may do so only accordance with applicable State and Federal Laws. Requests for access and copying must be in writing and signed by the patient or legal representative unless during a period of active care. This Policy and Procedure establishes the process for handling patient requests, circumstances where the Ponderosa Family Care may deny access, the patient's right to appeal a denial, the time frame within which requests will be processed, and fees for making requested copies available.

Generally speaking, a patient's medical record (whether paper, electronic document management, electronic health record (EHR) or defined hybrid systems and billing records contained within the designated record set) is used to provide inspection, copying and amendment of information. Because these records are compilations and summaries of information from other Source Systems and are in fact copies of other existing data and document types, they will be primarily offered for individual access, restriction and amendment.

PATIENT ACCESS TO PHI DURING AN EPISODE OF CARE

Pertinent information may be provided to patients and their personal representatives to share with other providers for treatment purposes. Patients may review their medical records (without addition or correction) during the period of active care. Corrections or additions must be handled in accordance with the administrative policies for 'Patient Request for Amendment of Protected Health Information'. The patient's attending provider should be notified if the patient has questions about the documentation or feels that information may be in error. These disclosures do not require authorization or written request. Access to Behavioral Health records should be handled in accordance with this Individual Access to PHI policy and with the guidance of the provider(s).

PATIENT ACCESS TO PHI AFTER PATIENT HAS CONCLUDED THE EPISODE OF CARE

1. Information available to the patient.

   Upon appropriate written request, access will be permitted to the individual patient's PHI, primarily medical records and billing records unless the information falls into one of the

categories which may be denied as discussed below. Peer review, quality assurance, and information created and maintained for business purposes of the Ponderosa Family Care and not used to make decisions about an individual patient in the process of healthcare delivery are not considered part of the designated record set and are not subject to review or copying by the patient or legal representative.

In addition, patients may not have the right to access and obtain copies of:

A. Psychotherapy Notes
B. Information compiled for use in civil, criminal, or administrative actions
C. Information subject to prohibition by the CLIA; or
D. Information that is not part of the designated record set.

2. Request must be in writing

Individual patients or legal representatives must request access to their own protected health information in writing. The request must be signed and dated by the patient or legal representative. Electronic forms and signature may be used in palce of paper forms and handwritten signatures.

3. Time frame for response to patient request

Access to inspect medical and billing records will be provided within five (5) working days of receipt of the written request. Copies will be provided within fifteen (15) working days of receipt of the written request.

4. Manner of access

The Ponderosa Family Care will arrange with the individual a convenient time and location in the facility to inspect or obtain copies of the PHI. Individuals reviewing records must provide identification upon request.

Inspection will be attended by a Ponderosa Family Care workforce member. The patient or legal representative will be referred to the patient's provider for discussion of clinical questions. Copies of the records may be mailed in lieu of inspection at the facility upon patient request.

5. Fees

No fee will be charged for retrieving a patient's records and allowing the patient or his legal representative to review them.

Reasonable cost-based fees (also per State mandated fee schedules) may be charged by the Ponderosa Family Care for providing copies of PHI, other than those requests delineated as no charge within appropriate published fee schedules or policy.

The fees will include the costs of copying paper records or printing for electronic records (including supplies and labor) and postage (if the individual has requested that the records be mailed). A current fee schedule will be provided upon request. Storage media may not be charged for.

6. Denial of patient access

A request for access or copies may be denied in the following situations:

A. The request is for records that are not available for inspection.
B. The Ponderosa Family Care is for records that are not available for inspection.
C. The PHI has been created or obtained during an active research project and the patient agreed that access would not be permitted while the research project was active;
D. The PHI contains information obtained from someone other than a healthcare provider under a promise of confidentiality and the requested access would reveal the source of the information;
E. The requested information has been compiled in anticipation of a civil, criminal, or administrative proceeding;
F. The request is for behavioral health records, which may contain reference to another person, and the Medical Director for Behavioral Health Services has determined that the information may endanger the life or safety of the patient or the other person referenced; or
G. The request is from the patient's legal representative for behavioral health records which makes reference to another person, and the Medical Director for Behavioral Health Services has determined that access to the information is likely to endanger the life or safety of such other person.
H. If access or copies are denied, a written explanation of the basis for denial will be provided to the patient or legal representative within five (5) working days of receipt of the request. This explanation will include information regarding whether or not an appeal to the Ponderosa Family Care may be made, the process for placing and handling such an appeal, and how to register a complaint with the Secretary of the Department of Health and Human Services.

7. APPEAL OF DENIAL

If access is denied, it must first be determined whether the denial may be appealed;

A. Unreviewable grounds for denial-

No appeal process exists under State or Federal Law in the following circumstances;

A. The PHI is exempted from the right of access;
B. The Ponderosa Family Care is acting under the direction of a correctional institution to deny access to an inmate, and the information could jeopardize the health, safety, security, custody, or rehabilitation of the inmate, any officer, employee, or other inmates.
C. A patient's right to protected health information created or obtained in the course of research may be temporarily suspended while the research is in progress, provided the patient has

agreed to the denial of access when agreeing to participate. The right of access will be reinstated access would reveal the source of the information.

D. The PHI contains information obtained from someone other than a healthcare provider under a promise of confidentiality and the requested access would reveal the source of the information.

The individual may appeal a denial under the following circumstances:

A. The Medical Director has determined that the access is likely to endanger the life or safety of the individual;
B. The records contain reference to anther individual and the Medical Director has determined that the access is likely to endanger the life or safety of such other person; or
C. The request is made by the individual's legal representative and the Medical Director has determined that the access is likely to endanger the life or safety of the individual or another person.

1. Appeal for review of a denial of access

   If access is denied based on reviewable grounds, an appeal must be made in writing and signed and dated by the patient or legal representative who made the original request.

   If an appeal is made, the review must be performed within a reasonable period of time by a licensed healthcare professional designated by the organization who did not participate in the original decision to deny access.

   The reviewer will determine whether or not to deny access based on the items listed above under 'Reviewable grounds for denial.' The reviewer will promptly report his decision to the organization that will provide written notice to the individual of the determination and initiate any appropriate action.

2. Retention of documentation

   All documentation related to an individual's, or legal representative's, request for access, and any documentation related to a denial process, will be filed with the medical record and retained in accordance with the policy for retention of medical records for a minimum of at least six (6) years.

**Procedures for Patient Access to PHI**

All requests for access to PHI by an individual patient or legal representative will be assessed in accordance with this policy. Appropriate response will follow promptly.

1. Written request

   All requests for access of copies of protected health information must be in writing (or via permanent electronic form) and must be signed and dated (which can be via electronic methods) by the individual patient or legal representative. Incomplete requests will be considered invalid and will be returned to the requestor immediately.

2. Reply to request

   Unless denied, access to inspect medical, behavioral health, and billing records will be permitted within five (5) working days of receipt of the written request. Copies will be provided within fifteen (15) working days of receipt of the written request.

   Patient requests for access to behavioral health information will be referred to the Medical Director and the requestor will be so notified immediately upon receipt of the request.

   If access or copies are denied under conditions listed above in this policy, the Medical Director, Risk Manager, or designee, will be so notified. A written explanation of the basis for denial will be provided to the patient or legal representative within five (5) working days of receipt of the request.

3. The process for appeal

   Upon receipt of a written appeal for review of the denial of appropriate parties, or designee, will be notified.

   Administrative arrangements will be made promptly to secure the services of a licensed healthcare professional not previously involved in the denial process.

   The requestor will be notified promptly of the determination of the reviewer. If access is to be permitted, arrangements will be made to permit inspection within five (5) days of the determination. If copies are to be provided, the copies will be provided within fifteen (15) days of the determination.

4. Retention of documentation

   All documentation relating to the request, or any denial or appeal will be filed with the medical record and retained in accordance with the policy on retention of medical records.

5. Timeliness provision changed.

   A. The Final Omnibus Privacy Rule modifies the timeliness requirements for right to access and to obtain a copy of PHI to 30 days from the date of the request.
      i. OCR has removed the provision that permits 60 days for timely action when protected

health information for access is not maintained or accessible to the covered entity on-site.

ii. OCR has retained the provision that permits a covered entity a one-time extension of 30 days to respond to the individual's request;

6. With written notice to the individual of the reasons for delay and the expected date by which the entity will complete action on the request.

    i. Covered entities that spend significant time before reaching agreement on the electronic format for a response are using part of the 30 days permitted.

**Copies of Electronic Records**

1. The Privacy Rule requires that if an individual requests an electronic copy of PHI that is maintained electronically in one or more designated record sets, the CE must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or

    A. If not, in a readable electronic form and format as agreed to by the covered entity and the individual.
    B. In such cases, to the extent possible, we expect covered entities to provide the individual with a machine-readable copy of the individual's PHI.
        i. HHS/OCR considers machine-readable data to mean digital information stored in a standard format enabling the information to be processed and analyzed by computer.
        ii. For example, this would include providing the individual with an electronic copy of the PHI in the format of MS Word or Excel, text, HTML, or text- based PDF, among other formats.
        iii. If an individual requests a form of electronic copy that the covered entity is unable to produce, the covered entity must offer other electronic formats that are available. If the individual declines to accept any of the electronic formats that are readily producible by the covered entity, the covered entity must provide a hard copy as an option to fulfill the access request.
    C. If the designated record set includes electronic links to images or other data, the images or other data that is linked to the designated record set must also be included in the electronic copy provided to the individual.
    D. How and to what extent a BA is to support or fulfill a CEs obligation to provide individuals with electronic access to their records will be governed by the Business Associate Agreement between the CE and the BA.

2. PDF is recognized as a acceptable electronic format, although OCR remains technically neutral.

3. Hard copy is to be provided if the individual denies all formats of electronic offered by the CE.

4. CEs are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Minimum Necessary | | | Policy # | 718 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 5 | |
| Policy Section | HIPAA Policies | | | | |

**PURPOSE:**

When using or disclosing PHI or when requesting PHI from another Covered Entity, they will make reasonable efforts to limit PHI to the Minimum Necessary to accomplish the intended purpose of the use, disclosure, or request.

**POLICY:**

As a general rule, Ponderosa Family Care may not use, disclose, or request the entire medical record of a patient unless the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

Uses or disclosures that impermissibly involve more than the minimum necessary information may qualify as Privacy Breaches under Interim and Final HIPAA Privacy Rules. In contrast, a use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper Minimum Necessary procedures would not be a violation of the Privacy Rule.

One manner in which Minimum Necessary criteria can be met is by disclosing "limited data sets' that exclude the direct identifiers listed below as well as dates of birth and zip codes, for a total of 18 identifiers. The Privacy Rule allows a covered entity to de-identify data by removing all 18 elements that could be used to identify the individual or the individual's relatives, employers, or household members. Under the HIPAA Privacy Rule "identifiers" that must be removed include the following:

1. Names;

2. All geographic subdivision smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census;
   A. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
   B. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates

(including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

4. Telephone numbers;
5. Fax Numbers;
6. Electronic mail addresses;
7. Social Security Numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators
15. Internet Protocol address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and any other unique identifying number, characteristic, or code, except as permitted; and the CE does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

Note: Birthdates and Zip codes no longer qualify as exceptions to the requirement to perform Breach Determination as of September 23, 2013, upon implementation of the Omnibus Final Privacy Rule.

LIMITED DATA SETS

Limited Data Set is created by removing the identifiers listed above for the purpose for which the LDS was created. A LDS can be utilized to disclose records without PHI for research, public health, or healthcare operations. The Ponderosa Family Care workforce may not use or disclose a LDS until a Data Use Agreement with the recipient of the LDS has been obtained. All uses of a LDS will comply with the Minimum use. In accordance with the Ponderosa Family Care's Accounting of

Disclosures policy the LDS does not need to be recorded in the Accounting of Disclosure log or with any Accounting of Disclosures request.

MINIMUM NECESSARY APPLICABILITY

The Ponderosa Family Care's workforce shall use, disclose or request the minimum necessary amount of PHI in all situations except the following:

1. Disclosures to or requests by a health care provider for treatment;

2. Uses or disclosures made to the individual;

3. Uses or disclosures made pursuant to a valid, written patient authorization;

4. Disclosures to the Secretary of the U.S. Department of Health and Human Services or related entities such as the Office for Civil Rights, charged with HIPAA privacy and Security enforcement.

5. Uses or disclosures that are required by Law; and

6. To meet the requirements of HIPAA, such as for the content of standard transactions.

The following protocols are facilitated by Ponderosa Family Care's Privacy and Security Officer(s) relative to the Minimum Necessary rule:

1. Ponderosa Family Care shall identify persons (or classes of persons) within Ponderosa Family Care who need access to PHI to carry out their duties.

2. For each person (or classes of persons), the Ponderosa Family Care shall identify the category (or categories) of PHI to which access is needed and any conditions appropriate to such access.

3. Once persons within Ponderosa Family Care who need access to PHI and categories of information are identified, Ponderosa Family Care must make reasonable efforts to limit access only to such identified persons and such uses or disclosures only in such identified categories. With respect to System access, patient privacy will be supported through authorization, access, and audit controls and will be implemented for all systems that contain patient identifiable information. Within the permitted access, a staff member may only access information needed to perform his/her job duties.

4. For disclosures that are of a non-routine nature, Ponderosa Family Care's Privacy Officer:
   A. Will develop criteria and train the applicable staff to limit the PHI disclosed to the amount reasonably necessary to accomplish the purpose of the disclosure or request; and
   B. Have the applicable staff at the Ponderosa Family Care review requests for disclosure on an individual basis in accordance with such criteria.

5. Standard Policies and Procedures can cover 'routine and recurring' uses, disclosures and requests without need for any review. A process must exist for reviewing the non-routine events on an individual basis.

6. Ponderosa Family Care's staff may rely on a requested disclosure as the Minimum Necessary for the stated purpose (if reliance is reasonable under the circumstances) in the following situations:
   A. When making disclosures to authorized public officials if the requesting official represents that the information is the minimum necessary.
   B. When the information is requested by another CE
   C. When the information is requested by a professional who is a member of the Ponderosa Family Care workforce, or is a BA of the Ponderosa Family Care for the purpose of providing professional services to the Ponderosa Family Care if the professional represents that the information requested is the minimum necessary for the states purpose(s).
   D. When the information is requested for research purposes and the person requesting the information has provided documentation that requests specific information.

DE-IDENTIFICATION OF PHI

Ponderosa Family Care may disclose de-identified PHI as set forth in this policy. De-identified PHI is health information that does not identify an individual, and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Health information shall be considered de-identified if either of the de-identification procedures set forth below is followed. In addition, Ponderosa Family Care may use PHI to create de-identified health information or disclose PHI to a BA to create de-identified health information. Ponderosa Family Care may determine that health information is de-identified health information if the following conditions exist.

Statistical Methods

A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (a) determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and (b) documents the methods and results of the analysis to justify such determination; or

Safe Harbor

1. All eighteen (18) of the following identifiers of the individual or relatives, employers or household members of the individual are removed:
   A. Names;
   B. Geographic subdivisions smaller than a state, etc
   C. All elements of dates, except year, directly related to an individual date, admission date, discharge date, date of death; and for all ages over 89, all elements of date including year indicative of such sage, except that such ages and elements may be aggregated into a single

category of age 90 or older. Note, however, that for research or other studies relating to young children or infants, the Ponderosa Family Care may express age of an individual in months, day or hours;

D. Telephone numbers;
E. Fax numbers;
F. Electronic-mail addresses;
G. Social Security numbers;
H. Medical record numbers;
I. Health plan beneficiary numbers;
J. Account numbers;
K. Certificate/license numbers;
L. Vehicle identifiers and serial numbers, including license plate numbers;
M. Device identifiers and serial numbers;
N. Web universal resource locators;
O. Internet protocol address numbers;
P. Biometric identifiers including finger and voice prints;
Q. Full face photographic images and any comparable images; and
R. Any other unique identifying number, characteristic, or code; except the Ponderosa Family Care may assign a code or other means of record identification to allow the Ponderosa Family Care to re-identify information that was identified if:
   i. The code or other means of record identification is not created from information about the individual and cannot be translated to identify the individual; and
   ii. The Ponderosa Family Care does not use or disclose the code or other means of record identification for any other purpose and does not disclose the method by which to re-identify the individual. HHS has removed the exception for limited data sets that do not contain any dates or birth dates and zip codes. In the Omnibus Final Rule, following the impermissible use or disclosure of any limited data set, a Covered Entity or BA must perform a risk assessment that evaluates the 4 'low probability of compromise' factors determine if breach notification is not required.

2. Ponderosa Family Care does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual patient who is a subject of the information.

In addition, a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified may be disclosed except as otherwise permitted under the Ponderosa Family Care's policies for disclosure of PHI.

De-identified information that has been re-identified may not be disclosed or used except as otherwise permitted under the Ponderosa Family Care's policies for use and disclosure of PHI.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Mitigation of Improper Use and Disclosure | | | Policy # | 719 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 2 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

To communicate the policy of the Ponderosa Family Care to prevent and respond to any improper use or disclosure of an individual's PHI.

## POLICY:

The Ponderosa Family Care mitigates, to the extent practicable, any harmful effect that is know, occurring as a result of a use or disclosure of PHI by the Ponderosa Family Care or any of its Business Associates, (BA) that is in violation of Ponderosa Family Care policies related to HIPAA Privacy and Security

Information regarding any suspected or actual inappropriate access, use or disclosure of PHI by the Ponderosa Family Care or any of its BAs that is discovered by any employee of the Ponderosa Family Care shall be forwarded promptly to the Ponderosa Family Care Privacy Officer. Suspected or actual inappropriate access, use or disclosure of PHI that has been reported will be termed a 'Privacy Event' and investigated as to whether a Privacy Violation or Breach occurred.

The Ponderosa Family Care's Privacy Officer, in response to such reports or other information regarding an unauthorized use or disclosure by the Ponderosa Family Care or any of its BAs, including self-disclosures made by BAs pursuant to the terms of each BA's contract or other agreement with the Ponderosa Family Care shall develop and implement a plan as soon as reasonably practicable to mitigate any known or reasonably anticipated harmful effects from such use or disclosure. The actions to mitigate such unauthorized use or disclosure shall be tailored to the circumstances of each case, but may include as appropriate, the following:

1. Identifying the source(s) of the use or disclosure and taking appropriate corrective action.

2. Contacting the recipient of the information that was the subject of the unauthorized disclosure and requesting that such recipient either destroy or return the information.

3. Instructing such recipient to make no further uses or disclosures of such information.

4. Depending on the circumstances, notifying the individual whose PHI was the subject of the unauthorized use or disclosure; and

5. Reviewing, and correcting where appropriate, any policy or procedure of the Ponderosa Family Care that directly caused or contributed to the unauthorized use or disclosure.

6. Remember that not all harm to a patient (individual) in the case of a Privacy Violation can be of an economic nature; there are other considerations, such as reputational hard, that will factor into the mitigation plan.

The Ponderosa Family Care's Security or Privacy Officer shall immediately notify, if appropriate, the Ponderosa Family Care's Legal Counsel, regarding the Security or Privacy Event, and/or the unauthorized use or disclosure of PHI and shall take further action as so advised. The Ponderosa Family Care Management and Legal Counsel shall determine, in the event that the unauthorized use or disclosure was made by a BA or Contractor, whether such disclosure warrants termination of the BA's contract. In addition, Ponderosa Family Care's Security or Privacy Officer shall notify the individual responsible for compiling accounting of disclosures so that any accounting can include the unauthorized use or disclosure, if appropriate.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Notice of Privacy Practices | | | Policy # | 720 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 3 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

The Privacy Rules provide that a patient, or his/her personal representative, has a right to receive a notice of the covered entity's privacy practices ("Notice of Privacy Practices or NPP"). The purpose of this policy is to describe the clinic's distribution, posting, and revising of that NPP.

## POLICY:

It is the policy of Ponderosa Family Care to:

1. Provide a copy of the NPP to all patients, or their representatives, no later than the date of their first date of service, or as soon as possible after an emergency situation;
2. Post a copy of the NPP in a clear and prominent location, or in multiple locations, in the clinic where it is reasonable to expect patients seeking care and services to be able to see and read the NPP;
3. Have copies of the NPP available for any patient who requests a copy;
4. Revise the NPP whenever a material change is required regarding PHI uses or disclosures, patients' rights, the clinic's privacy duties/obligations, or other privacy practices; and
    a. to distribute the revised NPP to all new patients at their first visit following the revision;
    b. to place the revised NPP on the clinic website; and
    c. to post at the clinic and to make available for any patient who requests a copy

## PROCEDURE:

1. An individual has a right to adequate notice of the uses and disclosures of PHI that may be made by the clinic, and of the individual's rights and clinic's responsibilities with respect to PHI. The clinic is required to provide a notice of privacy practices document to all patients, as well as other individuals requesting a copy. The front office staff will be responsible for distributing a copy of the notice to all patients.

2. The clinic will:
    A. Provide the notice no later than the date of the first service delivery, including service delivered electronically to such individual.
    B. Make a good faith effort to obtain an initial written acknowledgement of the receipt of notice from the patient on the Notice of Privacy Practices Acknowledgement Form.
    C. Have the notice available at the clinic for individuals to take with them.
    D. Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking care from the clinic to be able to read the notice.

E. Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision.

3. Exceptions
   A. If the clinic is treating patient during an emergency situation, the clinic does not have to provide a notice at the time of first service delivery. The clinic may delay the requirement for provision of notice and good faith effort of written acknowledgement.
   B. A prisoner receiving medical attention from the clinic does not have a right to receive a copy of the notice of privacy practices. However, the clinic must still protect prisoners' PHI.

4. Documentation of Notice
   A. The clinic must document compliance with the notice requirements by retaining copies of the notices issued by the clinic.
   B. Front office personnel will be responsible for distributing the notice to all patients and documenting the receipt of the Notice of Privacy Practices Acknowledgement form. (See Patient Index System).
   C. The original Notice of Privacy Practices Acknowledgement form will be filed in the patient's medical record.
   D. If a written acknowledgement was not obtained from the patient, the clinic must document the reason for the failure to obtain the written acknowledgement on the Notice of Privacy Practices Acknowledgement form.

5. Revision to the Notice

   The clinic must promptly revise and make available its notice whenever there is a material change to the uses or disclosures, the individual's rights, clinic's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

**Acknowledgement of Receipt of Notice of Privacy Practices**

I, _____ acknowledge that I have read and/or received a copy of Ponderosa Family Care Notice of Privacy Practices.

Date:_____ Witness:_____

**Failure to Obtain Signed Acknowledgment**

Date:_____

Ponderosa Family Care presented this Acknowledgment to _____. The patient refused to provide a signature when requested.

_____

Authorized Signature

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

Introduction:

At PONDEROSA FAMILY CARE, PLLC, we know that the privacy of your personal information is important to you. This notice describes how medical information about you may be used and disclosed & how you may gain access to this information and the measures taken to safeguard your information.

PONDEROSA FAMILY CARE, PLLC has established a policy to guard against unnecessary disclosure of your health information. For purposes of this notice, health information refers to any information that is considered protected health information as defined in the Privacy Rule of the Administrative Simplification provision of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Understanding Information Contained in Your Health Record

Each time you visit PONDEROSA FAMILY CARE, PLLC, a record of your visit is made. Typically this record contains dates of service, symptoms, diagnosis, examination and test results, medications given, treatment and plan for your future care. This information, referred to as your medical or health record serves as a:

- Basis for planning your care and treatment of your illness,
- Means of communication with other health professionals who contribute to your care,
- Legal document describing the care you received under our clinic,
- Means by which you or a third party payer can verify that services billed were provided and accurate,
- A tool in educating health care professionals,
- A source of data for medical research,
- Clinical guideline and protocol development, case management and care coordination.
- A tool with which we can access and study to work to improve the quality and effectiveness of the healthcare and service we provide and you receive.

Summary of Circumstances under Which You're Health Information May Be Used and Disclosed

To Make or Obtain Payment:

- We may use or disclose your health information to collect payment from third parties, such as health plans.

To Conduct Health Care Operations:

- PONDEROSA FAMILY CARE, PLLC, may disclose your health information for its own quality assurance operations.
- Contacting other health care professionals and providers with information about your treatment, alternatives and other related functions.

Copy Service:

- If we use a copy service for our health records when records requested by outside entities, be assured that our contracted business associates are required to properly safeguard your information.
- When legally require, we will disclose your health information when it is required to do so by any federal, state or local law.
- Federal law makes provision for health information to be released to an appropriate health oversight agency for authorized activities including audits, civil administrative or criminal investigations, inspections, licensure of disciplinary actions. In Connection with Judicial and Administrative Proceedings we may disclose health information in the course of any judicial or administrative tribunal as expressly authorized by such order or in response to a subpoena, discovery or other lawful process.
- Funeral director, only consistent with applicable law to carry out their duties.

In the Event of serious Threat to Health or Safety:

- We may, consistent with applicable law and ethical standards of conduct, disclose your health information if PONDEROSA FAMILY CARE, PLLC, in good faith, believes that such disclosure is necessary to prevent or lessen a serious and imminent threat to your health or safety or to the health and safety of the public.

For Workers Compensation:

- PONDEROSA FAMILY CARE, PLLC, may release your health information to the extent necessary to comply with laws related to Worker's Compensation or similar programs.

Notification and Communication with family:

- We may use any disclosure information to notify or assist in notifying a family member, personal relative, or another personal representative, or another person responsible for your care, your location, and general condition. Health professionals, using their best judgment may disclose to a family member, other relative, close family friend or any other person you identify, health information relevant to that person's involvement in your care or payment related to your care.

YOU'RE RIGHTS WITH RESPECT TO YOUR HEALTH INFORMATION

Your health care record is the property of PONDEROSA FAMILY CARE, PLLC; however the information belongs to you. You have the following rights regarding your health information that PONDEROSA FAMILY CARE, PLLC maintains.

Right to Request Restrictions

- You may request restrictions on certain uses and disclosures of your health information. However, PONDEROSA FAMILY CARE, PLLC, is not required to agree to your request.

Right to Inspect and Copy Your Health Information:

- You have the right to inspect and copy your health information. If you request a copy of your health information, we may charge a reasonable fee for copying, assembling costs and if applicable, postage associated with your request.

You have a right to amend your health record as provided in 45 CFR 164.528.

- If you believe that your health information records are inaccurate or incomplete, you may request that PONDEROSA FAMILY CARE, PPLC, amend your records. That request may be made as long as the information is maintained by PONDEROSA FAMILY CARE, PLLC.
- The request may also be denied if your health records were not created by PONDEROSA FAMILY CARE, PLLC, and is not part of our records.
- If the health information you wish falls within exception to the health information, you are permitted to inspect and copy, or if we determine the records containing your health information are accurate and complete.

You have the right to obtain:

- An accounting of disclosures of your health information as provided in 45 CFR 164.528.
- Request communications of your health information record by alternative means or at alternative location. Request a restriction on certain uses and disclosures of your health information record as provided by 45 CFR 164.528.
- Revoke your authorization to use or disclose your health information except to the extent that action has already been taken.

DUITES AND RESPONSIBILITIES OF PONDEROSA FAMILY CARE, PLLC

PONDEROSA FAMILY CARE, PLLC, is required by law to maintain the privacy of your health information as set forth in this notice and to provide to you this Notice of its duties and privacy practices. PONDEROSA FAMILY CARE, PLLC, is required to abide by the terms of this Notice, which may be amended from time to time. We reserve the right to change the terms of this notice and to make the new Notice provision effective for all health information we maintain. If PONDEROSA FAMILY CARE, PLLC, revises this notice we will provide you a copy of the revised Notice within 60 days of the change.

CONTACT INFORMATION

For more information or for further explanation of this document, you may contact the Privacy Officer: (PONDEROSA FAMILY CARE, PLLC, front office receptionist). You have the right to express complaints about PONDEROSA FAMILY CARE, PLLC, to the Secretary of the Department of Health and Human Services if you believe your privacy rights have been violated. We encourage you to express any concerns you may have regarding the privacy of your information. You will not be retaliated against in any way for filing a complaint.

The Address for the Office of Civil Rights is:

Office of Civil Rights
U.S. Department of Health and Human Services
200 Independence Avenue, S.V.
Room 509F, HHH Building
Washington, D.C. 20201

EFFTECTIVE DATE:
This notice is effective September 1, 2010

PONDEROSA FAMILY CARE, PLLC

Consent to the Use and Disclosure of Health Information for
Treatment, Payment or Healthcare Operations

I, _____ understand that as part of my healthcare, this practice originates and maintains health records describing my health history, symptoms, examination, diagnosis, treatment, medications, test results and any plans for my future care and treatment.

I have received a copy of this office's Notice of Privacy Practices that outlines how patient confidential information will be used, disclosed and protected and what my rights are concerning the information contained in my health information record.

_____ _____

Printed Patient Name

Name/Relationship if Signed by
Individual other than Patient

_____ _____

Signature

Date

For Office Use Only

An written acknowledgement of receipt of Notice of Privacy Practices was attempted but could not be obtained because:

_____Individual refused to sign

_____Individual was unable to sign

_____Verbal ok to sign was given

_____Communication Barrier

_____Care was Emergent

_____Other

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Patient Rights and Responsibilities | | | Policy # | 721 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 1 | |
| Policy Section | HIPAA Policies | | | | |

**PURPOSE:**

To ensure that rights of patients are protected.

**POLICY:**

It is the policy of Ponderosa Family Care that no patient shall be deprived of any rights, benefits, or privileges guaranteed by law, while a patient at the clinic.

**PROCEDURE:**

1. Prior to, or at the time of registration, the patient shall be fully informed of their rights.

2. The Statement of Rights shall be provided, or read to the patient in a language the patient can understand.

3. The following patient rights are adhered to at all times in the clinic:
   A. A patient is provided with care and services in the least restrictive environment.
   B. An individualized treatment plan is initiated and periodically reviewed in collaboration with the patient, and when appropriate, the family.
   C. A qualified professional is responsible for overseeing the implementation of this treatment plan.
   D. The patient, (patient's family, and/or legal guardian, as appropriate) are informed of the grievance procedure and how to lodge a complaint regarding a violation of their rights according to state law.
   E. Patient rights complaints are logged and include date, nature of complaint, and resolution. The administrator will maintain the log.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Patient Right to Amend PHI | | | Policy # | 722 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 3 | |
| Policy Section | HIPAA Policies | | | | |

**PURPOSE:**

To assure compliance that supports HIPAA regulations.

**POLICY:**

It is the policy of Ponderosa Family Care to secure and maintain the medical records of each and every patient receiving clinic services.

**PROCEDURE:**

1. Patients have a right to amend information collected and maintained about them in their designated record set (e.g. medical record and billing records).

2. All employees must strictly observe the following standards:
   A. A patient has the right to have the clinic amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.
   B. The clinic may deny a patient's request for amendment, if it is determined that the PHI or record that is the subject of the request:
      i. Was not created by the clinic, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment.
      ii. Is not part of the designated record set;
      iii. Is accurate and complete; or
      iv. Is not available for inspection as defined in policy.
   C. The patient must make the request to amend the PHI in writing with a reason to support a requested amendment. The request should be on the "Request for Correction/Amendment of Protected Health Information" form.
   D. The clinic must accept all requests to amend PHI in the designated record set; however, the clinic is not required to act on the patient's request if it is in accordance with item (b).
   E. The clinic must act on the patient's request for an amendment no later than 60 days after receipt of such a request. If the clinic is unable to act on the amendment within the required 60 day time limit, the clinic may extend the time for such action by no more than 30 days, provided that:
      i. The clinic provides the patient with a written statement of the reasons for the delay and the date by which action on the request will be completed.
      ii. The clinic may have only one such extension of time for action on a request for an amendment.
   F. If the amendment is granted, in whole or in part, the clinic must:

i. Make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.
ii. Inform the patient in a timely manner that the amendment is accepted and obtain the patient's identification of and agreement to have the clinic notify the relevant persons with which the amendment needs to be shared.
iii. Make reasonable efforts to inform and provide the amendment within a reasonable time to:
   a) Persons identified by the patient as having received PHI about the patient and needing the amendment.
   b) Persons, including business associates that the clinic knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeable rely, on such information to the detriment of the patient.

G. If the requested amendment is denied, in whole or in part, the clinic must provide the patient with a timely, written denial. The denial must use plain language and contain:
   i. The clinic must permit the patient to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The clinic may reasonably limit the length of a statement of disagreement.
   ii. The clinic may prepare a written rebuttal to the patient's statement of disagreement. Whenever such a rebuttal is prepared, a copy of the rebuttal must be provided to the patient who submitted the statement of disagreement.
   iii. The clinic must, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the patient's request for an amendment, the denial request, the patient's statement of disagreement, if any, and the rebuttal, if any, to the designated record set.

H. For future disclosures
   i. If a statement of disagreement has been submitted by the patient, the clinic must include the patient's request for an amendment, the denial of the request, the patient's statement of disagreement and the rebuttal, if any, or an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates.
   ii. If the patient has not submitted a written statement of disagreement, the clinic must include the patient's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI only if the patient has requested such action.
   iii. When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included with the disclosure, the clinic may separately transmit the material required to the recipient of the standard transaction.

3. Patients may request to have their PHI amended by submitting a Request for Correction/Amendment of Protected Health Information Form to the Practice Administrator. All requests to amend PHI will be reviewed by the Practice Administrator and appropriate provider.

4. The Practice Administrator has the authority to amend or correct any PHI that is administrative in nature. Any PHI that is clinical in nature must be amended by a consensus of the Medical

Director and primary care provider. Once a decision has been reached, the Practice Administrator will send a final letter outlining their decision to the patient Practice Administrator will be responsible for documenting the administrative decision and making the necessary changes, if applicable, to the PHI in the medical record. The Medical Director will be responsible for documenting the clinical decision and making the necessary changes, if applicable, to the medical record.

5. If the clinic is informed by another provider or payer of an amendment they have made to a patient's PHI within the outside entities' designated record set, the clinic must amend the PHI in the designated record set that have been received from those outside entities. The clinic does not have to amend the PHI in the clinic's designated record set based upon an outside determination, unless the clinic has relied on the outside entities findings.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Permitted Use and Disclosure | | | Policy # | 723 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 13 | |
| Policy Section | HIPAA Policies | | | | |

**PURPOSE:**

To assure compliance that supports HIPAA regulations.

**POLICY:**

It is the policy of Ponderosa Family Care to secure and maintain the medical records of each and every patient receiving clinic services.

**PROCEDURE:**

1. Definition:

   Protected Health Information (PHI) – Individually identifiable health information transmitted or maintained in any form or medium, including oral, written, and electronic. Individually identifiable health information relates to an individual's health status or condition, furnishing health services to an individual or paying or administering health care benefits to an individual. Information is considered PHI where there is a reasonable basis to believe the information can be used to identify an individual.

2. The clinic employees may use and disclose PHI for Treatment, Payment and health Operations (TPO). However, this only allows the clinic and its employees to use and disclose the "Minimum Necessary" amount of information required to complete the desired task.

3. Use with respect to individually identifiable health information: The sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

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

5. Treatment: The provision, coordination, or management of health care related services by one or more health care providers, 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 for the referral of a patient for health care from one health care provider to another.

6. Payment: Any activities undertaken either by a health plan or by a health care provider to obtain premiums determine or fulfill its responsibility for coverage and the provision of benefits or to

obtain or provide reimbursement for the provision of health care. These activities include but are not limited to:

A. Determining eligibility, and adjudication or subrogation of health benefit claims.
B. Risk adjusting amounts due based on enrollee health status and demographic characteristics.
C. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care processing.
D. Review of healthcare services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges.
E. Utilization review activities, including pre-certification and preauthorization services, concurrent and retrospective review of services.
F. Disclosure to consumer reporting agencies of certain PHI relating to collection of premiums or reimbursement.

7. Health care operations: Any one of the following activities to the extent the activities are related to providing health care:
   A. Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting patients with information about treatment alternatives, and related functions that do not involve treatment.
   B. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to clinic or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities.
   C. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance of health benefits, securing, or placing a contract for reinsurance of risk relating to claims for health care.
   D. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs.
   E. Business planning and development, such as conducting cost management and planning related analysis related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or covered policies.
   F. Business management and general administrative activities: Management activities related to HIPAA compliance, Customer Service, Resolution of internal grievances, Sales, transfer, merger, or consolidation of covered entities, Creating de-identified health information or limited data set, and fundraising for the benefit of the clinic.

8. Minimum Necessary: When using or disclosing PHI or when requesting PHI from another health care provider or health organization, the clinic must limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. Minimum Necessary does not apply in the following circumstances:
   A. Disclosure by a health care provider for treatment (students and trainees are included as health care providers for this purpose).

B. Uses and Disclosures based upon a valid consent to use and disclose PHI for treatment, payment and health care operations or a valid authorization to use and disclose PHI.
C. Disclosures made to the Secretary of Health and Human Services.
D. Uses and disclosures required by law.
E. Uses and disclosures required by other sections of the HIPAA privacy regulations.

9. Indirect Treatment Relationship: A relationship between an individual and a health care provider in which:
   A. The health care provider delivers health care to the individual based on the orders of another health care provider.
   B. The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services, products or reports to the individual.

10. Acknowledgements: Except in an emergency treatment situation, the clinic must make a good faith effort to obtain a written acknowledgement of receipt of the Notice of Privacy clinic, and if not obtained, document good faith efforts to obtain such acknowledgement and the reason why the acknowledgement was not obtained.

11. The clinic may use and disclose PHI for:
   A. Its own treatment, payment, or healthcare operations.
   B. Treatment activities of a health care provider.
   C. The payment activities of another cover or healthcare provider.
   D. The health care operation activities of another covered entity or health care provider, if each entity has or had a relationship with the individual who is the subject of the PHI being requested, and the disclosure is:
      i. For a purpose listed in the definition of health care operations.
      ii. For the purposed of health care fraud and abuse detection or compliance.
   E. Another covered entity that participates in an organized health care arrangement with the clinic for any health care operation activities of the organized health care arrangement.

12. Psychotherapy notes are not to be included as PHI that may be disclosed, unless authorization is obtained for such use of disclosure.

**FOR HEALTH OVERSIGHT REPORTING**

1. The clinic may disclose PHI without an authorization 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. Government benefits programs for which health information is relevant to beneficiary eligibility;
   B. Entities subject to government regulatory program for which health information is necessary for determining compliance with program standards;

C. Entities subject to civil rights law for which health information in necessary for determining compliance.

2. The following is NOT to be considered health oversight activity:
   A. The individual is the subject of the investigation or activity, and the investigation or other activity is not directly related to:
      i. The receipt of health care;
      ii. A claim for public benefits related to health (e.g. claims for Food Stamps);
      iii. 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. If a health oversight activity or investigation is related to a claim for public benefits not related to health, the joint activity or investigation shall be considered a health oversight activity for purposes of this policy.

4. The clinic is not considered to have violated the requirements of this policy, with just cause, if an employee who is the victim of a criminal act discloses PHI of the suspected perpetrator to a law enforcement official, provided that:
   A. The PHI disclosed is about the suspected perpetrator of the criminal act; and
   B. The PHI disclosed is limited to:
      i. Name and address.
      ii. Date and place of birth.
      iii. Social Security number.
      iv. ABO blood type and rh factor.
      v. Type of injury.
      vi. Date and time of treatment.
      vii. Date and time of death, if applicable.
      viii Description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars and tattoos.

**FOR JUDICIAL OR ADMINISTRATIVE PROCEEDINGS.**

1. Patient Health Information may be used or disclosed for judicial or administrative proceedings if the use or disclosure is made in response to a court order, administrative tribunal order, subpoena, discovery request, or other lawful process. The Practice Administrator will be notified of all requests.

2. The clinic may use or disclose PHI in the course of any judicial or administrative proceeding if:
   A. The disclosure is in response to an order of a court or administrative tribunal, provided that the clinic discloses only the PHI expressly authorized by such order; or
   B. In response to a subpoena, discovery request, or other lawful process, that is not a court order or administrative tribunal, if:
      i. The clinic receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to ensure that the subject of the requested PHI has been given notice of the request (with an affidavit from the requesting party); or

ii. The clinic receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the following requirements:
   a) Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and
   b) Requires the return to the clinic or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

C. The clinic receives satisfactory assurances from a party seeking PHI along with a written statement and accompanying documentation demonstrating that:
   i. The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location in unknown, to mail a notice to the individual's last known address);
   ii. The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and
   iii. The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:
      a) No objections were filed; or
      b) The court or the administrative tribunal has resolved all objections filed by the individual and the disclosures being sought are consistent with such resolution.
   iv. The clinic receives satisfactory assurances from a party seeking PHI including a written statement and accompanying documentation demonstrating that:
      a) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
      b) The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.
   v. Notwithstanding this section, the clinic has the option to disclose PHI in response to lawful process without receiving full satisfactory assurance, if the clinic of its own accord makes reasonable efforts to: provide notice to the individual sufficient to meet the requirements of this section or to seek a qualified protective order.

## PHI TO FAMILY & FRIENDS/INDIVIDUAL CARE AND NOTIFICATION PURPOSES

1. The clinic may use and disclose certain PHI without the written consent or authorization to release the information from the individual. The individual must be informed in advance of the use or disclosure and have the opportunity to agree, prohibit, or restrict the disclosure. The clinic may orally inform the individual of the permitted uses and disclosures and obtain the individual's agreement or objection to a use or disclosure permitted by this policy. The clinic staff must document the agreement, prohibition, or restriction in the medical record. In some circumstances, the clinic may use and disclose certain information without consent, authorization, or oral agreement.

2. The clinic may disclose to a family member, other relative, 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 care or payment related to the individual's health care. The clinic may use or disclose PHI to notify or to assist in the notification of 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. The clinic can also use and disclose PHI in these circumstances for identifying or locating the types of persons mentioned above. In order for the clinic to use or disclose PHI for these purposes, the individual's presence is a determining factor. The following processes outline how the clinic may use and disclose PHI for these purposes.

3. If the individual is present for or otherwise available prior to, a use or disclosure and has the capacity to make health care decisions, the clinic may use and 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.
   C. Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does object to such disclosure.

4. 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 clinic may, in 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 health care. The clinic may use professional judgment and its experience with common clinic to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up X-rays or other similar forms of PHI.

**TO HEALTH AND HUMAN SERVICES**

1. The clinic may use or disclose PHI to the U.S. Department of Health and Human Services (HHS), if necessary to determine whether the clinic is in compliance with HIPAA Privacy Standards.

2. A person who believes clinic personnel are not complying with required HIPAA privacy standards may file a complaint with HHS. The following are requirements for filing complaints. Complaints must:
   A. Be in writing, either on paper or electronically.
   B. Name the clinic as the subject of the complaint and describe the acts or omissions believed to be in violation.
   C. Filed within 180 days of when the complainant knew or should have known that the act or omission occurred.

3. clinic personnel must keep proper records and upon request of HHS submit compliance reports whereby HHS can ascertain whether the clinic has complied with the HIPAA privacy standards. Any requests from HHS must be forwarded to the Practice Administrator. During an

investigation or review, clinic personnel must cooperate with HHS and permit access to the following information:

A. Facility, books, records, accounts, and other sources of information, including PHI, that is pertinent to ascertaining compliance with requirements (If HHS determines that serious circumstances exist, clinic personnel must permit access by HHS at any time and without notice.)
B. If any information required of the clinic is in the exclusive possession of any other agency, institution, or person and the other agency, institute, or person fails or refuses to furnish the information, the clinic must so certify and set forth what efforts it has made to obtain the information.

**FOR PUBLIC HEALTH AND SAFETY**

1. Definition:

   Disclosure – Means the release, transfer, provision of access to, or divulgence in any other manner, of information to any organization external to the clinic.

   Use – Means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within the clinic.

2. The clinic may disclose PHI without a patient authorization:
   A. For reporting of abuse, neglect, or domestic violence.
   B. To avert a serious and imminent threat to the health or safety of a person or the public.
   C. When allowed by law.

3. The clinic 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.

4. The clinic must meet the requirements pertaining to the disclosure relating to: victims of abuse, neglect, or domestic violence; judicial and administrative proceedings; and disclosures for law enforcement purposes.

5. 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 clinic, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims.
      ii. If the individual is unable to agree because of incapacity, a law enforcement or other public official may authorize to receive the report if:
         a) The PHI sought is not intended to be used against the individual.

b) 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.

D. In making a permitted disclosure, the clinic must promptly inform the individual, in the exercise of professional judgment, that such a report has been or will be made, except if:
   i. The clinic believes informing the individual would place the individual at risk of serious harm.
   ii. The clinic would be informing a personal representative, and the clinic 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 clinic.

6. Serious Threat to the Health or Safety of the Public
   A. The clinic may, consistent with applicable law and standards of ethical conduct, use or disclose PHI, if:
      i. The clinic, in good faith believes 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; except a use and disclosure may not be made if the information is learned by the clinic.
         b) Except a use and disclosure may not be made if the information is learned by the clinic.
            - In the course of treatment which, is designed to alter or change the desire to commit the criminal conduct which would be the basis for making a disclosure.
            - When an individual initiates or is referred to the clinic for treatment, counseling, or therapy.
      ii. Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.
   B. It 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 clinic reasonably believes may have cause serious physical harm to the victim.
      ii. Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.
   C. Limitations and Good Faith related to the Serious Threat

The clinic may only release the statement relating to the serious threat and the PHI related to the serious threat. If the clinic acts in good faith upon its belief, then the clinic will be protected for disclosures related to the serious threat.

7. Law Enforcement Purposes
   A. The clinic can only disclose PHI pursuant to a court order or subpoena.
   B. Identification and Location Purposes
      i. The clinic may disclose PHI in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material

witness, or missing person, provided that the clinic only discloses the following information:

ii. Name and address
iii. Date and Place of Birth
iv. Social security number
v. ABO blood type and rh factor
vi. Type of injury
vii. Date and time of treatment
viii. Date and time of death, if applicable
ix. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos.

C. Except as permitted in the paragraph above, the clinic may not disclose for the purposes of identification or location under that paragraph of this section any PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

8. Victims of a Crime
   A. The clinic may disclose PHI in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to this section, if:
      i. The individual agrees to the disclosure.
      ii. The clinic is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provider that:
         a) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim.
         b) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.
         c) The disclosure is in the best interests of the individual as determined by the clinic, in the exercise of professional judgment.

9. Crime on Premises
   A. The clinic may disclose to a law enforcement official PHI that the clinic believes in good faith constitutes evidence of criminal conduct that occurred on site.

10. Reporting Crime in Emergencies
    A. A clinic health care provider providing emergency health care in response to a medical emergency, other than such emergency on site, may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement:
       i. The commission and nature of a crime.
       ii. The location of such crime or of the victim(s) of such crime.
       iii. The identity, description, and location of the perpetrator of such crime.
    B. If a clinic health care provider believes that the medical emergency is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care any

disclosure to a law enforcement official for law enforcement purposes is subject to the Abuse, Neglect or Domestic Violence section of this policy.

## FOR MARKETING

1. Clinic personnel may not disclose, use, sell or coerce an individual to consent to the disclosure, use, or sale of PHI for marketing purposes without the authorization of the patient or personal representative who is the subject of the PHI. This prohibition includes the disclosure, use or selling of prescription drug patterns. Certain marketing activities such as face-to-face communication made by the clinic to the individual or promotional gift of nominal value provided by the clinic do not require the clinic to obtain patient authorization for the use of disclosure of PHI.

2. Clinic personnel shall not disclose PHI to any non-affiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer, unless the patient has authorized the disclosure. A clinic authorization form must be obtained for marketing purposes. The content of the form may not be altered. If marketing is expected to result in direct or indirect remuneration to the clinic from a third party, the clinic must state the remuneration in the authorization form.

3. If the marketing communication is not face-to-face but in written form, the clinic must make a determination prior to sending out the marketing communication that the product or service being marketed may be beneficial to the health of the patient. The clinic is required to send envelopes to the patient that has only the addresses of the sender and the recipient and must:
   A. State the name and toll free number of the clinic or clinic affiliated entity sending the marketing information.
   B. Explain clearly the recipient's right to have his/her name removed from the sender's mailing list.
   C. If the clinic or clinic affiliate for marketing purposes receives patient's request for removal from the mailing list, such removal must occur immediately, within FIVE days of receipt of request.
   D. The clinic must explain in the communication why the patient has been targeted and how the product or service relates to their health.

## BASED ON PATIENT AUTHORIZATION

1. Confidentiality of health information is the right of each patient seeking health care through the clinic. All protected health information (both written and verbal) is strictly confidential. Use and disclosure of PHI based on patient authorization shall be done only after completion of a valid authorization and obtaining the patient's signature.

2. A valid authorization must contain at least the following elements and must be written in plain language:
   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 or class of persons, authorized to make the requested use of disclosure.
C. The name or other specific identification of the person or class of persons, to whom the clinic may make the requested use or disclosure.
D. Description of each purpose of the requested use and disclosure. The statement "at the request of the individual" is sufficient description when an individual initiates the authorization and does not, or elects not to, provide a statement of purpose.
E. A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization.
F. A statement that the information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by the HIPAA Privacy Regulations.
G. Signature of the individual and the date.
H. If a personal representative of the individual signs the authorization, a description of individual's authority to act for the individual.
I. If the authorization is for marketing the clinic must include a statement acknowledging if direct or indirect remuneration is given to the clinic.
J. The authorization may contain elements or information in addition to the required elements, provided that such additional elements or information are not inconsistent with the required elements.

3. An authorization for use and disclosure of PHI may not be combined with any other document to create a compound authorization, except for the following:
   A. An authorization for the use or disclosure of PHI created for research that includes the treatment of the individual may be combined as permitted by the HIPAA Research Policies.
   B. An authorization for the use and disclosure of psychotherapy notes may only be combined with another authorization for use and disclosure of psychotherapy notes.

4. The clinic may not condition treatment on an authorization except in the event of:
   A. Provision of research-related treatment upon receiving an authorization for such research.
   B. Provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on the provision of an authorization to such third party (e.g., for life insurance or disability evaluation).

5. An authorization is considered defective and invalid if any material information in the authorization is known to be false by the clinic or its employees or if any of the following defects exist:
   A. The expiration date has passed or the expiration event is known by the covered entity to have occurred
   B. The authorization has not been filled out completely with respect to an element described as a core element.
   C. The authorization is known by the covered entity to have been revoked.
   D. The authorization violates the compound authorizations requirement or the prohibition of authorizations requirement.

E. Any material information in the authorization is known by the clinic to be false.

**FOR DISASTER PURPOSES**

1. The clinic 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 purposes of coordinating with such entities.

**FOR SPECIALIZED GOVERNMENT FUNCTIONS**

1. Clinic personnel may not disseminate PHI, unless the individual to whom the PHI belongs, and a valid authorization has been obtained requests it. PHI may be used or disclosed without authorization for specialized government purpose. The Practice Administrator should be contacted for verification of individuals representing a specialized government agency such as:
   A. Armed Forces personnel, the Red Cross, or other authorized agents of the Armed Forces, if deemed necessary by appropriate military command.
   B. Authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities.
   C. Authorized federal officials for the provision of protecting the President or foreign heads of state.
   D. The Department of State to make medical suitability determinations.
   E. A correctional institution or a law enforcement official with lawful custody of an inmate if necessary for the health and safety of such individual, other inmates, officers, or other employees at the correctional institution.
   F. Governmental programs providing public health benefits and governmental agencies administering such programs.

2. The clinic may use and disclose the PHI of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command.

3. The clinic may use and disclose the PHI of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the same guidelines that apply to US Armed Forces.

4. The clinic may disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by law.

5. The clinic may disclose PHI to a correctional institution or law enforcement official having lawful custody of an inmate or other individual PHI, if the institution or official represents that such PHI is necessary for:
   A. The provision of health care to such individuals.
   B. The health and safety of such individual or other 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 individuals and officer or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another.

E. Law enforcement on the premises of the correctional institution.
F. The administration and maintenance of the safety, security, and good order of the correctional institution.

6. Any component of the clinic that is affiliate with a correctional institution may use PHI of individuals who are inmates for any purpose of which such PHI may be disclosed.

7. For the purpose of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

8. Any clinic health plan that is a government program providing public benefits may disclose PHI to another agency either to enroll or determine member eligibility.

9. The clinic when administering a government program that provides public benefits may disclose PHI to another covered entity that is a like agency as long as the programs serve the same or similar populations and the disclosure of PHI is necessary to coordinate the covered functions of such program or to improve administration and management relating to the covered function of such program.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Photographs, Video Recordings, Audio Recordings, and Other Imaging of Patients | | | Policy # | 724 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 3 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

The purpose of this policy is to establish guidelines for situations where patients and/or workforce members may or may not be photographed, video or audio recorded, or otherwise imaged within Ponderosa Family Care and its clinics.

Definitions:

- **Audio Recording**: recording an individual's voice using video recording (e.g., video cameras, cellular telephones, tape recorders, or other technologies capable of capturing audio).

  **Video Recording**: Recording of both the visual and audible components (e.g., video cameras, cellular telephones, and other technologies capable of capturing both audio and visual images)

  **Photography**: recording an individual's likeness (e.g., image, picture) using photography (e.g., cameras, cellular telephones), video recording (e.g., video cameras, cellular telephones), digital imaging (e.g., digital cameras, web cameras), or other technologies capable of capturing an image (e.g., Skype).

## POLICY:

1. It is the policy of Ponderosa Family Care that photographs, video recordings, audio recordings or other imaging of patients, will be treated as Protected Health Information (PHI) in accordance with the HIPAA Privacy Rule.

2. Employees who use or disclose patient photography or recordings will comply with all applicable HIPAA policies and procedures, including but not limited to, Permitted Use and Disclosure Policy.

3. Ponderosa Family Care and its employees are strictly prohibited from photographing, video or audio recording patients or the patient's visitors within Ponderosa Family Care for personal use, including but not limited to taking pictures to share with friends and/or co-workers, or to post on the internet using social media (i.e., Facebook, Snap Chat, Twitter, etc.)

4. Ponderosa Family Care will take reasonable steps to protect patients, visitors, and workforce members from unauthorized photography, video or audio recordings or other images.

## PROCEDURE:

### Written Patient Consent Required

- Security camera may be in use that may capture patients in hallways. A sign stating that security cameras are in use in hallways will be posted at the entrance.

- Informed consent will ALWAYS be obtained from patients or their legal guardians PRIOR to photographing, imaging or audio recording a patient in exam rooms, with few exceptions.

    - *Exception*: Photographs may be taken by employees of Ponderosa Family Care to document abuse or neglect of a minor or incompetent adult with the consent of the patient or his/her legally authorized representative. Such photographs may be submitted with the required report to the investigating agency, but they should not be used for other purposes (such as teaching) without authorization.

    - *Exception*: Employees may take photographs of patients for medical/legal purposes after verbal permission is obtained and documented in the medical record.

### Family and Friends

- Permission must be obtained from the patient before the patient's family and friends photograph or videotape them in the Ponderosa Family Care or premises. Written consent of other patients is required if they will be in the photographs or videotape. This is required in order to protect their privacy rights. If staff notices a visitor, patient or family member taking photographs or videotaping other patients, they should be asked to immediately stop and erase photographs or videotapes if they do not have the written consent of the patient. If the person fails to stop the filming, Security should be contacted.

### News Media

- In general, facilities may permit, <u>but are not required</u>, to permit news media to photograph or audio record a patient, if the patient consents and the patient's responsible (*e.g.,* attending) physician agrees the patient is medically and psychologically stable. Due diligence must be maintained to ensure that other patients, who have not signed a consent, are not photographed or recorded and that there is no perception that they have been recorded.

### Maintenance of Photography, Video, Audio or other recording:

- Prior to erasure or destruction, all photographs, videotapes and other images should be stored in a manner that ensures timely retrieval when requested. Patient privacy and confidentiality of all patient images should be maintained.

### Disclosure:

- Photographs and audio recordings should not be released without specific written authorization from the patient, unless the disclosure is for treatment, payment or health care operations purposes or is otherwise permitted or required by law or as directed by court action.

- Unless prohibited by law, prior to erasure or destruction all photographs and audio recordings may be released to the patient in accordance with Patients' Right to Access when the information is part of the designated record set.

**Records Management**

- Facilities must retain the originals in accordance with state law and the Records Management Policy. Security camera images and video from hallways and common areas may be destroyed on a regular basis based on the size limits of the storage files and need for security investigations. Access to Security footage will only be available to the Administrator or physician in charge.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Printing or copying of PHI | | | Policy # | 725 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 1 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

To assure compliance that supports HIPAA regulations.

## POLICY:

It is the policy of Ponderosa Family Care to secure and maintain the medical records of each and every patient receiving clinic services.

## PROCEDURE:

1. Printed versions of PHI should not be copied indiscriminately or left unattended and open to compromise.

2. Printers and copiers used for printing of PHI should be in a secure location.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Privacy Complaint | | | Policy # | 726 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 1 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

To assure compliance that supports HIPAA regulations.

## POLICY:

It is the policy of Ponderosa Family Care to secure and maintain the medical records of each and every patient receiving clinic services.

## PROCEDURE:

1. Any individual who believes the rights granted by the Health Insurance Portability and Accountability Act (HIPAA) privacy regulations or any other state or federal laws dealing with privacy and confidentiality have been violated may file a complaint regarding the alleged privacy violation.

2. Any privacy related complaint made by a patient, employee, or student at anytime must be forwarded to the Practice Administrator. Complaints may also be made anonymously be calling the clinic. The Practice Administrator will investigate the alleged privacy violations. The Practice Administrator will also investigate any applicable information technology systems to determine if a breach of privacy has occurred.

3. If during the course of investigation an individual is found to be in violation of a clinic policy, he/she will be subject to the disciplinary process.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Privacy Risk Assessment | | | Policy # | 727 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 2 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

The purpose of this policy is to provide guidance on the process of an initial then ongoing assessment of the Ponderosa Family Care's privacy risk analysis which will create items for remediation. The stated purpose for this regular privacy risk analysis is to reduce the risk of privacy events, incidents or breaches to an acceptable level, while assisting with the Ponderosa Family Care overarching HIPAA security and privacy rule compliance program.

## POLICY:

This policy is intended to provide the basis for assessment of privacy risks within the Ponderosa Family Care and to provide a list of items that need to be addressed through remediation of the identified privacy risks, in a reasonable and appropriate manner. Assessment of Privacy risks and compliance with HIPAA Privacy and Security Rules is a continual process, with repeated assessments as computer networks and systems change or workflow processes are updated. The entire Privacy Risk Assessment should be reviewed and re-assessed yearly to ensure maximum compliance.

The results of the Ponderosa Family Care's Privacy Risk Assessment will be incorporated into our risk management plan (program). Periodic reviews of Ponderosa Family Care's security policies, procedure and technologies will be included within our ongoing risk management and assessment process.

Our Privacy Risk Assessment is intended to meet the requirements contained with HIPAA, from both privacy and security perspectives; and, for evaluating items to be remediated and managed. Performing a Privacy Risk Assessment is more of a general requirement than the more regulated Security Risk Analysis which is called for within the HIPAA Security Rule as well as the Meaningful Use program. Privacy Risk Assessments are emphasized as crucial to successful compliance programs; therefore, the Ponderosa Family Care considers our Privacy Risk Assessment to be as important as Security Risk Assessments.

All privacy risk assessments activities shall be documented and kept, as with all other HIPAA documentation, for six (6) years from its creation or last revision date, whichever is later.

It is the policy of the Ponderosa Family Care to conduct a regular Privacy Risk Assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the PHI we create and maintain. Whenever changes to technology or procedures occur, there may be changes to privacy and security risks and vulnerabilities. The Ponderosa Family Care will reassess and update

policies and procedures according to the results of the assessments and may include new/additional employee training if deemed necessary.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Request to Restrict Use & Disclosure of PHI | | | Policy # | 728 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 3 | |
| Policy Section | HIPAA Policies | | | | |

**PURPOSE:**

To define the process by which an individual can restrict the subsequent disclosure of certain PHI for payment and operations.

**POLICY:**

Section 164.522(a) of the Privacy Rule requires Covered Entities to permit individuals to request that a Covered Entity restrict uses or disclosures of their protected health information for treatment, payment, and health care operations purposes, as well as for disclosures to family members and certain others permitted under 164.510(b).

In the case that an individual requests that a Covered Entity restrict the disclosure of the protected health information of the individual, the Covered Entity must comply with the requested restriction if—

1. Except as otherwise required by Law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes carrying out treatment): and

2. The protected health information pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

Individuals requesting restrictions to the disclosure of their PHI must submit a written request form. Written requests should only be accepted after an individual pays the entire balance of the billing for the service or item for which restriction for payment or operations is requested. The Covered Entity should discuss the process with the individual requesting the restriction so that they clearly understand the requirement of having the item or service paid for out of pocket and at $0 balance before this restriction request must be honored.

HIPAA does not require the Ponderosa Family Care to agree to a restriction requested by an individual except in limited cases where the item or service has been paid out of pocket and in full; any acceptance by Ponderosa Family Care to agree to a restriction will only consider the addition of restrictions on disclosure in very limited circumstances as determined on a case-by-case basis.

EXCEPTIONS TO RESTRICTIONS

If in the event Ponderosa Family Care has agreed to restrict the use or disclosure of PHI, Provider shall not use or disclose the restricted PHI in violation of such restriction except that:

1. To facilitate treatment, and

2. Ponderosa Family Care may use or disclose restricted PHI, if such use or disclosure is permitted or required under Ponderosa Family Care policies relative to research and patient registries.

TERMINATING A RESTRICTION

If Ponderosa Family Care has agreed to restrict the use or disclosure of PHI, Ponderosa Family Care may terminate its agreement to restrict its use or disclosure of such PHI if:

1. The individual agrees to or requests the termination in writing.

2. Ponderosa Family Care informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI about the individual created or received after Ponderosa Family Care has so informed the individual;

3. Ponderosa Family Care discovers the agreement for restriction of use or disclosure for payment or operations for item or service paid out of pocket by an individual was not actually completely paid to a zero balance for that item or service.

Ponderosa Family Care shall document any restriction in the patient's medical record and such restriction will also be documented in the appropriate tracking system. Ponderosa Family Care shall maintain such documentation for six (6) years from the date when the restriction was last in effect.

AGREEMENT TO RESTRICTION EXCEPTION FOR EMERGENCY TREATMENT

A Covered Entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restrictions is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual. (iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

DOWNSTREAM NOTICE OF RESTRICTIONS

The Ponderosa Family Care is only required to maintain restrictions to the uses or disclosures of PHI under regulatory requirements or as agreed upon with the individual to whom the PHI applies. The Ponderosa Family Care does not have a responsibility to notify other providers of care on legitimate uses of the PHI about the restrictions, that being solely the individual's responsibility. The Ponderosa Family Care will engage in open dialogue with individuals to ensure that they are aware that previously restricted PHI may be disclosed to the health plan unless they request an additional restriction and pay out of pocket for the follow-up care.

EXCEPTION FOR MEDICARE AND MEDICAID

There is an exception to the right of restriction such as mandatory claim submission provisions under Medicare and similar requirements under Medicaid.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Revocation of Use & Disclosure | | | Policy # | 729 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 1 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

To assure compliance with a patient's right to revoke a previously granted authorization to release his/her PHI.

Background: A patient authorization is required where we seek to use, obtain, or release PHI for purposes other than treatment, payment or health care operations or for situations not addressed by an exception under HIPAA. In such instances, patients will generally be required to read and sign an authorization form prior to the use, release or request of their PHI.

A patient may revoke previously granted authorizations at any time, provided that the revocation is in writing. The revocation of an authorization will be effective immediately, except to the extent that we have taken action in reliance on the authorization or if the authorization was obtained as a condition of obtaining insurance coverage where other law provides the insurer with the right to contest a claim under the policy.

## POLICY:

It is the policy of Ponderosa Family Care that patient revocations of authorization are made in writing to the clinic on a Revocation Form and, once all necessary information is received, the revocation is processed in a timely and thorough manner.

## PROCEDURE:

1. An individual may revoke an authorization at any time, provided that the revocation is in writing, unless the clinic has already provided PHI based on the patient's authorization.

2. The Revocation Form should be used.

3. The clinic will stop providing information based on a patient's authorization as soon as possible.

4. The clinic will not be liable for a use or disclosure of a patient's PHI after a revocation, if the clinic in good faith based its actions upon a prior authorization and has already acted in reliance upon the authorization.

5. The completed Revocation Form must be given to the Privacy Officer with a copy to the Practice Administrator for proper documentation in the medical record.

## Ponderosa Family Care

## Revocation of Authorization for Use and/or Disclosure of Protected Health Information

| Patient Name: | |
|---|---|
| Social Security or Account Number: | Date of Birth: |

1. I hereby acknowledge that I have previously given my written Authorization to Ponderosa Family Care ("the Clinic") to use or disclose:

   (a) the following health information (*provide a detailed description*):

   _____
   _____
   _____

   (b) for the following purpose(s) (*provide a detailed description*):

   _____
   _____
   _____

   (c) on _____ (*date*)

   which I now revoke.

2. I understand that the revocation of my Authorization will be effective immediately, except to the extent that:

   - Ponderosa Family Care has taken action in reliance thereon;
   - My Authorization was obtained as a condition of obtaining insurance coverage, where other law provides the insurer with the right to contest a claim under the policy or the policy itself; or
   - In the case of a research study, my health information is necessary to maintain the integrity of the study.

**BY SIGNING BELOW, I ACKNOWLEDGE THAT I HAVE READ THIS FORM AND UNDERSTAND THE TERMS AND CONDITIONS OF REVOKING MY AUTHORIZATION.**

_____ _____

Signature of Patient or Patient's Representative Date

_____

Printed Name of Patient's Representative (*if applicable*)

_____

Representative's Relationship to Patient *(if applicable)*

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Sanctions Enforcement and Discipline | | | Policy # | 730 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 5 | |
| Policy Section | HIPAA Policies | | | | |

**PURPOSE:**

To define the Policy and Procedures to be followed for Enforcement and Discipline (also known as 'Sanctions') related to HIPAA Security and/or Privacy Violations and Breaches.

**POLICY:**

ENFORCEMENT AND DISCIPLINE

Sanctions, or disciplinary action for workforce members (Employees) and Contractors who have failed to comply with the Ponderosa Family Care policies and procedures, or federal and state laws, or those who have otherwise engaged in conduct that has the potential of impairing the Ponderosa Family Care status as a reliable, honest and trustworthy entity, is an important part of privacy policy and procedures relating to PHI Privacy and Security. Therefore, all Employee and Contractors are required to acknowledge adherence to these policies and procedures as a material condition of employment or contracting with the Ponderosa Family Care. Failure to comply with these policies and procedures will result in discipline up to and including immediate termination.

The Ponderosa Family Care has this policy of progressive discipline (sanctioning) for employee wrongdoing, except where immediate termination is identified as the penalty. Disciplinary action may include remedial training, oral warnings, written reprimands, suspension and termination. Contractors can be terminated or sanctioned or otherwise disciplined according to their Business Associate agreement and/or contract terms. Whether the violation is a result of simple negligence, gross negligence, or an intentional act will be considered in determining the appropriate penalty.

If an Employee or Contractor has committed an infraction which would otherwise require discipline or termination, the Employee or Contractor may nevertheless be subject to a lesser punishment at the sole discretion of the Owner, Secretary, or administrator of the LLC.

Appropriate disciplinary action will depend upon: (i) the nature of the activity; (ii) whether the violator could reasonably be expected to identify the activity as a non-violation; (iii) whether the violator was in a position to take appropriate corrective action; (iv) whether the violator was unduly influenced to participate in the activity; and (v) any past violations or wrongdoings by the violator. Additionally, the decision to terminate an Employee or Contractor or to impose a lesser sanction will be influenced by: (i) whether the Employee or Contractor promptly reported their own violation; (ii) whether the report constitutes the Ponderosa Family Care's first awareness of the violation and the Employee's or Contractor's involvement; and (iii) whether the Employee or Contractor cooperates fully in investigating and correcting the violation.

To ensure consistency and to monitor the effectiveness of the Security and Privacy Policies and Procedures, every violation or wrongdoing subject to disciplinary action must be reported to the owner. Based upon a reported event, the Ponderosa Family Care's Security or Privacy Officer, after consultation with Ponderosa Family Care's chain of command. Any Ponderosa Family Care employee subject to disciplinary action under these policies and procedures will have appeal rights consistent with those in his or her employment agreement, or in the Ponderosa Family Care personnel manual, as applicable.

Effective security and privacy compliance programs include procedures to discipline employees who fail to detect wrongdoing as well as those who commit the wrongdoing. Accordingly, the Ponderosa Family Care will handle security and privacy violations as set forth in this policy, and any others that are applicable, concerning disciplinary action for security and privacy violations. The imposition of any disciplinary action or penalty under the Ponderosa Family Care's security or privacy policies and procedures will not waive the Ponderosa Family Care's right to seek monetary damages or to otherwise enforce its legal rights against the disciplined Employee or Contractor.

1. Management's Responsibility for Discipline
   The chain of command shall ensure that the Ponderosa Family Care establishes procedures for the discipline of workforce members for violation of the security and/or privacy policies and procedures.

2. Privacy as an Element of Performance Reviews
   Security and Privacy policy and procedures require that the promotion of, and adherence to their included elements be a factor in evaluating the performance of Ponderosa Family Care's Employees and Contractors. They will be periodically trained in new privacy policies and procedures. In addition, all managers and supervisors involved in the access, use and disclosure of PHI will:
   A. Discuss with all of their supervised Employees and Contractors the Ponderosa Family Care's policies and legal requirements applicable to their function.
   B. Inform all of their supervised personnel that strict compliance with these policies and requirements is a condition of employment.
   C. Disclose to all supervised personnel that the Ponderosa Family Care will take disciplinary action up to and including termination for violations of these policies and requirements.
   D. Managers and supervisors will be disciplined appropriate for failure to adequately instruct their subordinates, or for failing to detect noncompliance with applicable policies and legal requirements, where reasonable diligence on the part of the manager or supervisor would have led to the earlier discovery of any problems or violations and would have provided the Ponderosa Family Care with an opportunity to correct them.

3. Record and Reporting of Disciplinary Actions
   The Security and Privacy Officers shall maintain a record of all disciplinary actions involving security or privacy and report at least annually to the Ponderosa Family Care's management regarding such actions.

## RESPONDING TO DETECTED OFFENSES AND DEVELOPING CORRECTIVE ACTION PLANS

The purpose of this policy is to set forth the procedures to be used by the Ponderosa Family Care to respond to reports by Ponderosa Family Care workforce members (including employees and contractors) that an individual or individuals affiliated with or employed by the Ponderosa Family Care have discovered a Security or Privacy Event (or Incident) that may represent a violation of HIPAA or State Law, Rule or Standards. This policy cannot control procedures utilized by the Ponderosa Family Care's affiliate Business Associates, but should be addressed with each BA as a part of the Business Associate Agreement.

## PURPOSE OF PRIVACY EVENT INVESTIGATIONS

The purpose of a Security or Privacy Investigation is to:

A. Identify those situations in which the Laws, Rules and Standards of the HIPAA and the Ponderosa Family Care's security and privacy policies may not have been followed.
B. Identify individuals who may have knowingly or inadvertently caused PHI security/privacy to be managed in a manner which violated Laws, Rules and Regulations of HIPAA and State privacy Laws, Rules and Regulations;
C. Facilitate the correction of any practices not in compliance with security and privacy Laws, Rules and Regulations and
D. Implement those procedures necessary to ensure future compliance;
E. Protect the Ponderosa Family Care in the event of civil or criminal enforcement actions; and
F. Preserve and protect the Ponderosa Family Care's assets.

## CONTROL OF SECURITY AND PRIVACY EVENT INVESTIGATIONS

The respective Security and Privacy Officer(s) are responsible for directing the investigation of the alleged event, problem or incident. Reports of investigations shall be presented to the chain of command. At the discretion of the Chain of command, if a Security or Privacy Event Investigation reveals intentional, criminal, or reckless conduct, a report may be forwarded to Legal Counsel in which event Legal Counsel shall be responsible for directing the investigation of the alleged problem or incident. In undertaking an investigation, the Security or Privacy Officer or Legal Counsel may solicit the support of internal audit, external counsel and auditors, and internal and external resources with knowledge of the applicable Laws and Regulations and required policies, external resources with knowledge of the applicable Laws and Regulations and required policies, procedures or standards that relate to the specific problem in question. These individual's shall function under the direction of the Security or Privacy Officer or Legal Counsel and are required to submit relevant evidence, notes, findings and conclusions to the Security or Privacy Officer (as appropriate) or Legal Counsel depending upon who is directing the investigation.

## PRIVACY EVENT INVESTIGATIVE PROCESS

Upon receipt of a complaint or other information (including audit results) which suggest the possible existence of a pattern of conduct in violation of privacy policies or applicable Laws, Rules or Regulations, a Privacy Event Investigation(under the direction and control of the Privacy Offer or Legal Counsel as necessary), shall be commenced as soon as reasonably possible. Steps to be followed in undertaking the Investigation include, but need not be limited to:

1. An interview of the complainant and other persons who may have knowledge of the alleged problem or process and a review of the applicable Laws, Rules and Regulations which might be relevant to or provide guidance with respect to the appropriateness or inappropriateness of the activity in question, to determine whether or not a problem actually exists.
2. The identification and review of the situation to determine the nature of the problem, the scope of the problem, the frequency of the problem, the duration of the problem and the potential financial magnitude of the problem.
3. Interviews of the person or persons who appeared to play a role in the process which caused the problem. The purpose of the interview is to determine the facts related to the complained of activity, and may include, but is not limited to:
   A. Personal understanding of the HIPAA and State Laws, rules and Regulations.
   B. The identification of persons with supervisory or managerial responsibility in the process.
   C. The adequacy of the training of the individuals performing the functions within the process.
   D. The extent to which any person knowingly, or with reckless disregard or intentional indifference, acted contrary to the HIPAA or State Laws, Rules or Regulation.
   E. The nature and extent of potential civil or criminal liability of individuals or the Ponderosa Family Care and
   F. Preparation of a summary report which shall indicate at a minimum:
      i. Defines the nature of the problem;
      ii. Summarizes the Investigation process;
      iii. Identifies any person whom the investigator believes to have either acted deliberately or with reckless disregard or intentional indifference toward the HIPAA or State Laws, Rules and Regulations.
      iv. If the review results in conclusions or findings that the conduct referenced in the complaint is permitted under applicable Laws, Rules or Regulations or Policy or that the complained of act did not occur as alleged or that it does not otherwise appear to be a problem, the Investigation shall be closed.
      v. If the initial Investigation concludes that there has been a HIPAA or State Law, Rule or Regulations violation, or that additional evidence is necessary, the investigation proceeds to the next step.

CORRECTIVE ACTIONS

If at the conclusion of an Investigation involving a Security or Privacy issue it appears that there are genuine compliance concerns, the Security or Privacy Officer shall immediately formulate and implement a Corrective Action Plan. The Security or Privacy Officer shall obtain the advice and guidance of Legal Counsel and approval of the chain of command in formulating and implementing the Corrective Action Plan. The Corrective Action Plan shall be designed to ensure that the specific issue is addressed and, to the extent possible, that similar problems do not occur in other departments

or areas. The Security or Privacy Officer shall document the corrective action taken by using the appropriate forms and documentation procedures.

1. Possible Criminal Activity. If the investigation reveals possible criminal activity (conduct which is intentional, willfully indifferent, or with reckless disregard for the Law), the Ponderosa Family Care shall:
   A. Immediately stop the activity related to the problem until the offending practice is corrected;
   B. Initiate appropriate disciplinary action against the person or persons whose conduct appears to have been intentional, willfully indifferent, or with reckless disregard for the Law,
   C. Make such notification to any Federal (Office for Civil Rights-OCR for HIPAA) or State Regulatory or Prosecutorial Authorities as Legal Counsel advises; and
   D. Promptly undertake an appropriate program of education to prevent future similar problems.
2. Other Noncompliance: If the investigation reveals noncompliant conduct which does not appear to be intentional, willfully indifferent, or with reckless disregard for the Law, the Ponderosa Family Care shall the above steps also apply.
   A. Monitoring

Any issue for which a Corrective Action Plan is implemented shall be specifically targeted for monitoring and review as part of future audits.

PREVENTION

If a Security or Privacy Event Investigation points out a systemic deficiency in the Ponderosa Family Care's policies or procedures or standards or if there have been similar incidents previously, the Security or Privacy Officer, with the advice of Legal Counsel and the approval of the chain of command, will recommend and institute appropriate changes to the applicable policies, procedures and training programs to prevent the problem from recurring, and privacy policies and procedures will be amended accordingly. The Security or Privacy Officer will review the record of the Investigation and the pertinent privacy policies and procedures, and may interview personnel and examine other documents to determine what additional steps need to be implemented to avoid similar future violations. All workforce members or Contractors will be promptly notified of any resulting changes to the Security or Privacy policies, procedures and standards.

EDUCATION

All workforce members shall be educated and trained at new hire and on a routine basis on the Sanctions, Enforcement and Discipline related to privacy and security violations. Documentation of this education shall be maintained along with other privacy and security training.

LEGAL COUNSEL

Where appropriate, the Security or Privacy Officer shall consult with the Ponderosa Family Care's Counsel regarding the appropriate corrective action to be taken for a violation.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Security of Medical Records | | | Policy # | 731 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 3 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

To ensure that the clinic and its officers, employees, and agents have the necessary medical and other information to provide the highest quality medical care possible while protecting the confidentiality of that information to the highest degree possible so that patients do not fear to provide information to the clinic and its officers, employees and agents for purpose of treatment.

## POLICY:

It is the policy of Ponderosa Family Care to secure and maintain the medical records of each and every patient receiving clinic services.

## PROCEDURE:

1. Collect and use individual medical information only for the purposes of providing medical services and for supporting the delivery, payment, integrity, and quality of those services. The clinic and its officers, employees, and agents will not use or supply individual medical information for non-health care uses, such as direct marketing, employment, or credit evaluation purposes other than as authorized by the Health and Human Services Privacy Regulations.

2. Collect and use individual medical information only:
   A. To provide proper diagnosis and treatment.
   B. With the individual's knowledge and consent/authorization.
   C. To receive reimbursement for services provided.
   D. For research in similar purposes designed to improve the quality and to reduce the cost of health care.
   E. As a basis for required reporting of health information.

3. Recognized that medical information collected about patient must be accurate, timely, complete, and available when needed. The clinic and its officers, employees, and agents will:
   A. Use their best efforts to ensure the accuracy, timeliness, and completeness of data and to ensure that authorized personnel can access it when needed.
   B. Complete and authenticate medical records in accordance with the law, medical ethics, and accreditation standards.
   C. Maintain medical records for the retention periods required by law and professional standards.
   D. Not alter or destroy an entry in a record, but rather designated as an error while leaving the original entry intact and create and maintain a new entry showing the correct data.

E. Implement reasonable measures to protect the integrity of all data maintained about patience.

4. Recognized that patients have a right of privacy. The clinic and its officers, employees, and agents will respect patients' individual dignity at all times. The clinic and its officers, employees, and agents will respect patients' privacy to the extent consistent with providing the highest quality medical care possible and with the efficient administration of the facility.

5. Act as responsible information stewards and, treat all individual medical record data and related financial, demographic, and lifestyle information as sensitive and confidential. Consequently, the clinic and its officers, employees, and agents will:
   A. Treat all individual medical record data ("protected health information") as confidential in accordance with the HHS privacy regulations, other legal requirements, professional ethics, and accreditation standards.
   B. Only use or disclose the minimum necessary help information to accomplish the particular task for which the information is used or disclosed.
   C. Not divulge medical record data unless the patient (or his/her authorized representative) has properly consented to the release or the release is otherwise authorized by the privacy regulations and/or other law, such as communicable disease reporting, child abuse reporting, and the like.
   D. When releasing medical record data, take appropriate steps to prevent unauthorized three disclosures, such as specifying that the recipient may not further disclose the information without patient consent or as authorized by law.
   E. Implement reasonable measures to protect the confidentiality of medical and other information maintained about patients.
   F. Removed patient identifiers when appropriate, such as in statistical reporting and in medical research studies.
   G. Not disclose financial or other patient information except as necessary for billing or other authorized purposes as authorized by the privacy regulations, other laws, and professional standards.
   H. Recognize that some medical information is particularly sensitive, such as HIV/AIDS information, mental health and developmental disability information, alcohol and drug abuse information, and other information about sexually transmitted or communicable diseases and that disclosure of such information could severely harm patients, such as by causing loss of employment opportunities and insurance coverage, as well as the pain of social stigma. Consequently, the clinic and its officers, employees, and agents will treat such information with additional confidentiality protections as required by law, professional ethics, and accreditation standards.

6. Recognize that although the clinic "owns" the medical record, the patient has a right of access to information contained in the record. The clinic and its officers, employees, and agents will:
   A. Permit patients to access and copy the protected health information in accordance with the requirements of the privacy regulations.
   B. Provide patients an opportunity to request correction of inaccurate data in their records in accordance with the requirements of the privacy regulations.

C. Provide patients an accounting of uses and disclosures other than those for treatment, payment, and health-care operations in accordance with the requirements of the privacy regulations.

7. All officers, agents, and employees of the clinic must adhere to this policy. The clinic will not tolerate violations of this policy. Violation of this policy is grounds for disciplinary action, up to and including termination of employment.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Storage of Medical Records | | | Policy # | 732 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 1 | |
| Policy Section | HIPAA Policies | | | | |

**PURPOSE:**

To assure compliance that supports HIPAA regulations.

**POLICY:**

It is the policy of Ponderosa Family Care to secure and maintain the medical records of each and every patient receiving clinic services.

**PROCEDURE:**

1. All personnel must strictly observe the following standards relating to the storage of PHI:
   A. Outside of regular working hours, clinic personnel must clean desks and work areas such that all PHI is properly secured, unless the immediate area can be secured from unauthorized access.
   B. When not in use, PHI must always be protected from unauthorized access. When left in an unattended room, such information must be appropriately secured.
   C. If PHI is to be stored on the hard disk drive or other internal components of a personal computer or PDA (Personal Digital Assistant), it must be protected by either a password or encryption. Unless encrypted, when not in use, this media must be secured from unauthorized access.
   D. If PHI is stored on diskettes, CD-ROM or other removable data storage media, it cannot be commingled with other electronic information.

2. The Practice Administrator is responsible for enforcing this policy. Individuals who violate this policy will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.

127 E. Main Street, Suite D, Payson, AZ 85541 Phone: 928-978-3080

| Policy/Procedure Title | Training Workforce HIPAA | | | Policy # | 733 |
|---|---|---|---|---|---|
| Manual Location(s) | Ponderosa Family Care | Effective | 12/03/20 | Page 1 of 2 | |
| Policy Section | HIPAA Policies | | | | |

## PURPOSE:

This policy establishes the Ponderosa Family Care Security (and Privacy) Awareness Training Program in order to establish and promote the highest levels of security and privacy compliance and protections for all protected health information (PHI) accessed, used and disclosed by workforce members.

## POLICY:

The Ponderosa Family Care's Privacy and Security Officer(s) are responsible for providing direction and oversight of the provision of workforce privacy and security training.

The Ponderosa Family Care recognizes its status as a Covered Entity under the definitions contained in the HIPAA regulations and that it must comply with HIPAA regulations in references to the training of workforce members, in accordance with the requirements at 164.530(b) and 164.308(a)(5). The Ponderosa Family Care believes effective and complete HIPAA training programs, in combination with appropriate HIPAA resources, can significantly reduce the possibilities of HIPAA violations and breaches of confidential information. HIPAA training, at minimum, shall include the basics of HIPAA regulations and best practices; the basics of HIPAA's privacy and security requirements and restrictions; and review of relevant and appropriate policies and procedures related to HIPAA compliance. Regular messages and reminders in reference to HIPAA security awareness, as well as those related to privacy, will also be utilized. HIPAA awareness resources should strive to maintain a high level of HIPAA awareness amongst the workforce members, and a protective attitude toward confidential data on an ongoing, daily basis.

Workforce members will be trained a new hire positions. All workforce member training shall be tailored to job roles, responsibilities and access rights to PHI, including methods of and requirements for authentication (i.e. logons).

Workforce members shall have training annually or upon material changes introduced by regulation, if their duties are impacted by these regulations. Exceptions to these training time cycles may occur if material changes make additional training necessary during the time between regular training cycles and schedules. Also there may be requirements from OCR (Office for Civil Rights), State Agencies or other similar bodies that mandate additional or custom training. All additional training will be facilitated in compliance with requirements generated by that action.

Documentation of this training must be kept in an organized reproducible manner for a period of not less than six (6) years. Records of all workforce training shall be kept and produced upon request by regulators or other authorized parties.