



HIPAA  
Information Safety Management  
Program  
PRIVACY & SECURITY  
POLICIES & PROCEDURES

REVISED 10/08/19 by and approved by Privacy Officer Linda Grow

**PROHEALTH PARTNERS/  
ARGUS MEDICAL  
MANAGEMENT**

## **P-1000 General Administrative Policies and Procedures**

The policies in this section (P-1000) of the **ProHealth Partners** policy and procedure manual establish the medical practice's administrative policies and procedures for safeguarding the privacy of protected health information.

### **Regulation**

#### **45 CFR 164.530**

Establishes requirements for administrative measures to implement the policy standards.

## **P-1100 Staff Responsibilities**

The policies in this section establish the organizational responsibility for compliance with the privacy standards and for overseeing the efforts of **ProHealth Partners** to safeguard the privacy of patient information.

### **Regulation**

#### **45 CFR 164.530(a)**

Requires designation of a privacy official and contact person responsible for policy development and handling of privacy inquiries and complaints.

#### **45 CFR 164.514(d)(2)**

Requires identification of the categories of protected health information that each class or category of staff member may use or disclose.

### ***Information Classification:***

***Sensitive data*** includes all human resource data, financial data, Practice proprietary information, and personal health information ("PHI") protected by the Health Insurance Portability and Accountability Act ("HIPAA").

### **PHI includes:**

- Names
- Addresses
- Geographic subdivisions smaller than a state
- All elements of dates directly related to the individual (Dates of birth, marriage, death, etc.)
- Telephone numbers
- Facsimile numbers
- Driver's license numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers, certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers

- Full face photographic images and any comparable images

**Sensitive data in the form of PHI resides on:**

- CareTracker (Over 100,000 patient records)
- Paper Records (Printed, Fax, Mail, Medical Records)
- On-Site Network Attached Storage Unit
- Mobile Storage Units (Storage drives taken off-site for backup)

- **Handling of PHI:**

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by the Argus Medical Management and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of Argus Medical Management policy and will result in personnel action, and may result in legal action.

All employees must have up-to-date documented HIPAA training prior to accessing PHI.

All data records on CareTracker are considered PHI, and protected under HIPAA.

All records on Argus FTP server are considered to contain PHI, and protected under HIPAA.

No PHI is allowed on the public network drive or folder at any time unless in approved encrypted form and with documented authorization by HIPAA Security Officer.

No PHI is allowed on network drives without documented authorization from HIPAA Security Officer.

No PHI is ever allowed to be exported from CareTracker or any other computer workstations unless the workstation is encrypted, and authorized by HIPAA Security Officer.

- No *sensitive data* should ever be stored on transportable media unless the data is maintained in an encrypted format.
- Sensitive Data on hard copy should be handled with confidentiality, and properly locked and secured when not in use. Trash receptacles marked for shredding containing PHI should be emptied into locked bins for shredding at the end of each working day.
- All Policies in the HIPAA Privacy and Security manual regarding handling of PHI must be followed.
- All hardcopy medical records that are no longer used and/or to be shredded must never be left unsecured or unattended.

**Handling of Paper Records**

Record Retention - Documents relating to uses and disclosures, authorization forms, business partner contracts, notices of information practice, responses to a patient who wants to amend or correct their information, the patient's statement of disagreement, and a complaint record are maintained for a period of 6 years<sup>300</sup>.

Record Destruction - All hardcopy medical records that require destruction are shredded using NIST 800-88 guidelines.

## **P-1110 Designation of Privacy Official**

**Privacy Officer** is responsible for the development and implementation of policies and procedures to safeguard the privacy of patients' health information consistent with federal and state laws and regulations.

The specific responsibilities of **Privacy Officer** include:

- Developing policies and procedures as provided in policy P-1500
- Developing and conducting training programs on privacy policies and procedures
- Responding to questions from staff and patients concerning privacy policies and procedures
- Receiving complaints concerning the privacy practices described in the Notice of Privacy Practices (see policy P-3100)
- Auditing compliance with privacy policies and procedures
- Investigating and correcting violations of privacy policies and procedures

The **Privacy Officer** may assign any of these responsibilities to other staff members or contractors, but continues to be responsible for making sure these responsibilities are carried out.

### **Regulation**

#### **45 CFR 164.530(a)(1)**

Requires designation of a privacy official responsible for development and implementation of privacy policies and procedures and a contact person or office responsible for providing further information and receiving complaints about privacy practices.

## **P-1120 General Staff Responsibilities**

All staff are responsible for safeguarding the privacy of patient health information. Specific staff responsibilities under these privacy policies and procedures will be listed in the staff member's job description.

All staff members must:

- Use and disclose protected health information only as authorized in their job description or as authorized by a supervisor
- Conduct oral discussions of personal health information with other staff or with patients and family members in a manner that limits the possibility of inadvertent disclosures
- Complete privacy training prior to receiving access to protected health information. Employees will be re-trained annually (at a minimum) (See policy P-1200.)
- Report suspected violations of a business associate's contractual obligations to safeguard protected health information (See policy P-1400.)
- Report suspected violations of the policies and procedures established in this manual by staff members as detailed in policy P-1500

### **Regulation**

#### **45 CFR 164.514(d)(2)(ii)**

Requires reasonable efforts to limit access of workforce members to the classes of information necessary to carry out their duties.

## **P-1130 Authority and Responsibility of Individual Staff Members**

The job description of all staff members who require routine access to protected health information to perform their job-related duties must identify:

- The job functions that require the use or disclosure of protected health information

- The classes of protected health information that the position will use or disclose
- Any restrictions on the protected health information that the position can use or disclose
- The procedures that must be followed to use or disclose protected health information that is not routinely available to the position

These requirements may be satisfied by referring to standard job classes that the **Privacy Officer** may establish under policy P-2300 to define the positions authorized to routinely use or disclose standard categories of protected health information.

### **Regulation**

#### **45 CFR 164.514(d)(2)(ii)**

Requires reasonable efforts to limit access of workforce members to the classes of information necessary to carry out their duties.

### **P-1200 Staff Training**

This section establishes the responsibility for the development and updating of staff training programs and materials on privacy policies and procedures. It also establishes the responsibility of all staff members to complete privacy training.

### **P-1210 Content of Privacy Training Program for Staff**

The **Privacy Officer** or a staff member designated by the **Privacy Officer** will develop a privacy policy orientation and training program.

This purpose of this program is to make sure that all staff members are familiar with the privacy policies and procedures adopted by **ProHealth Partners** **prior to receiving access to protected health information.**

The training and orientation program will cover:

- The definition and identification of protected health information
- Providing the Notice of Privacy Practices to all patients and obtaining a written acknowledgment of receipt
- Using and disclosing protected health information for treatment, payment, and health care operations
- Obtaining authorization, when required, for use and disclosure of protected information
- Procedures for handling suspected violations of privacy policies and procedures
- Penalties for violations of privacy policies and procedures
- Documentation required by the policies and procedures manual

Staff members will:

- Receive a summary of the medical practice's privacy policies and procedures
- Have an opportunity to review the policies and procedures manual
- Have an opportunity to ask questions about the privacy policies and procedures of **ProHealth Partners.**
- **Complete form SF-1110 Attestation of HIPAA Privacy and Security Training and return form to HR.**

### **Regulation**

#### **45 CFR 164.530(b)(1)**

Requires training of all staff members on privacy policies and procedures.

### **P-1220 Initial Privacy Orientation and Training**

All staff members must complete the privacy policy orientation and training program **prior to receiving access to protected health information, and on-going training during** their probationary period. Completion of the privacy policy orientation and training program will be documented in the employee's personnel file by **Privacy Officer**, or the staff member who conducts the training. **Supervisors will closely monitor new employee's use and disclosure of protected health information during the probationary period.**

#### **Regulation**

##### **45 CFR 164.530(b)**

Establishes HIPAA requirements for staff training.

### **P-1230 Revised Policy and Procedure Training**

The **Privacy Officer** or a staff member designated by the **Privacy Officer** will develop training materials on new or revised privacy policies and procedures.

#### **Procedures**

- Staff whose job responsibilities are affected by a change in privacy policies and procedures must complete training on the revised policies and procedures within one month of their effective date.
- Completion of training on revised policies and procedures will be documented in the employee's personnel file.

#### **Regulation**

##### **45 CFR 164.530(b)(2)(ii)**

Requires documentation of training.

### **P-1300 Staff Compliance and Sanctions**

The policies in this section of the privacy manual establish disciplinary procedures for employees whose actions are out of compliance with **ProHealth Partners** privacy policies and procedures.

#### **Regulation**

##### **45 CFR 164.530(e)**

Requires covered entities to apply appropriate sanctions against staff members who violate its privacy policies and procedures.

### **P-1310 Reporting of Suspected Violations of Privacy Policies and Procedures**

All staff members should report possible violations of privacy policies and procedures to their supervisor. If the supervisor determines that a violation occurred, or that the situation warrants further investigation, the possible violation should be reported to the **Privacy Officer**.

Under the following circumstances, potential violations should not be reported by a staff member to his or her supervisor:

- When the violation involves the staff member's supervisor, it should be reported directly to **Privacy Officer**.
- When the violation involves the **Privacy Officer** it should be reported to the **ProHealth Board of Directors**.

- When the violation involves a member of the **ProHealth Board of Directors**, it should be reported to the secretary of Health and Human Services (HHS).

Reportable offenses include use and disclosure of protected health information that may violate:

- The practices described In the Notice of Privacy Practices form
- A patient’s authorization

Discussion of protected health information in public areas should be reported only if the discussion involves the disclosure of a substantial amount of protected health information and it would have been practical to conduct the discussion in a private area.

The staff member reporting a violation should briefly describe the possible violation in writing, or should arrange a meeting with the **Privacy Officer** to discuss the possible violation.

### **P-1311 Sanctions and Penalties**

There are two types of violations of privacy policies and procedures:

- Technical violations that do not result in the use or disclosure of protected health information
- Violations that do involve the use or disclosure of protected health information

There also are two types of violations that involve use and disclosure:

- Unintentional or accidental uses or disclosures
- Intentional and deliberate uses and disclosures

Incidental disclosures of information such as disclosures that occur when a patient asks a question in a public area, do not need to be reported, documented, or investigated. No sanction will be imposed for incidental disclosures of information. Staff members should, nevertheless, make reasonable efforts to minimize incidental disclosures.

The severity of penalties varies with the type of violation. The most severe penalties apply to the intentional disclosure of protected health information in violation of policies and procedures.

The least severe penalties apply to unintentional technical violations of policies that do not result in the disclosure of protected health information.

Examples of violations include:

- *Technical violations.* When obtaining an authorization, a staff member fails to notice that the patient signed but did not date the authorization form.
- *Accidental disclosure.* Information on the wrong patient is accidentally sent to a third-party payer.
- *Intentional disclosure.* A staff member provides a drug company representative a list of patients with an identified medical condition without obtaining the patients’ authorization for this disclosure.

The procedures and penalties that apply to each of these types of violation are defined in policies P-1312 through P-1315.

**Regulation**  
**45 CFR 164.530(e)**

Requires covered entities to apply appropriate sanctions against staff members who violate their privacy policies and procedures.

### **P-1312 Investigation of Potential Privacy Violations by Staff Members**

Upon being notified of a potential violation of privacy policies and procedures by a staff member or patient (under policy P-8000), the **Privacy Officer** will:

- Review any documentation
- Meet with the staff member or patient who reported the possible violation
- Meet with the staff member(s) who may have violated the policies and procedures
- Determine what, if any, protected health information was used or disclosed
- Determine whether the use or disclosure violated policies and procedures
- Determine whether the violation was accidental or intentional
- Recommend to the staff member's supervisor the disciplinary action, if any, that should be taken
- Document the findings of the investigation and action taken

#### **Regulation**

##### **45 CFR 164.530(e)**

Requires covered entities to apply appropriate sanctions against staff members who violate their privacy policies and procedures.

### **P-1313 Sanctions and Penalties for Technical Violations Not Involving Use and Disclosure**

A staff member who commits a technical violation of privacy policies and procedures that does not result in any use or disclosure of protected health information will:

- Meet with his or her supervisor to review the policies and procedures that were violated
- Demonstrate to the satisfaction of the supervisor that he or she understands the policies and procedures that should be followed in similar circumstances

The violation will be documented in the staff member's personnel file.

A pattern of repeated technical violations, even if none result in the inappropriate use or disclosure of protected health information, may result in transfer to another position, suspension, or termination of the staff member.

#### **Regulation**

##### **45 CFR 164.530(e)**

Requires appropriate sanctions against medical practice staff members who violate privacy policies and procedures.

### **P-1314 Sanctions and Penalties for Unintentional Violations Involving Use and Disclosure**

A staff member who unintentionally uses or discloses protected health information in violation of the privacy policies and procedures will:

- Meet with his or her supervisor to review the use or disclosure of protected health information that violated the medical practice's policies and procedures or the staff member's authority to use or disclose information

- Demonstrate to the satisfaction of the supervisor that he or she understands the uses and disclosures that he or she is authorized to make under the practice's policies and procedures

The violation will be documented in the staff member's personnel file.

A pattern of repeated unauthorized use or disclosure of protected health information will result in transfer to another position, suspension, or termination of the staff member.

#### **Regulation**

##### **45 CFR 164.530(e)**

Requires covered entities to apply appropriate sanctions against workforce members who violate its privacy policies and procedures.

### **P-1315 Sanctions and Penalties for Intentional Violations Involving Use and Disclosure**

The intentional violation of privacy policies and procedures may result in immediate suspension, pending further investigation and termination.

Documentation of the investigation of the violation must show clear evidence that the disclosure of information was *intentional and deliberate*. That is, the staff member must have disclosed the information *knowing* that the disclosure violated the policies and procedures of the practice.

If the staff member has previously disclosed the same or similar type of information under the same or similar circumstances, it will be presumed that the disclosure was intentional and deliberate.

#### **Regulation**

##### **45 CFR 164.530(e)**

Requires covered entities to apply appropriate sanctions against workforce members who violate its privacy policies and procedures.

### **P-1316 Protection of Whistleblowers**

No action shall be taken against a staff member who reports violation of privacy standards to the secretary of HHS or to law enforcement agencies.

##### **45 CFR 164.530(g)**

Prohibits a covered entity from retaliation against individuals who report violations of the privacy standards.

### **P-1320 Document of Sanctions Brought Against Employees**

The **Privacy Officer** shall establish and maintain files that document all actions taken to impose sanctions under policies P-1311 through P-1314. This information shall include:

- A description of, and documenting evidence for, the violation
- A statement clarifying the nature of the violation, specifically indicating whether it was technical or involved the use or disclosure of protected health information, and whether the violation of policies was accidental or intentional
- A description of the sanction that was imposed

An unproven or unsubstantiated allegation of a violation of privacy policies and practices does not have to be documented.

### **Regulation**

#### **45 CFR 164.530(e)(2)**

Requires covered entities to document sanctions that are applied.

### **P-1400 Business Associates and Protected Information**

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 or has access to PHI in a ProHealth Partners Office.

In short, any person (other than an employee or other member of the practice staff) or organization that receives or uses or has access to protected health information from **ProHealth Partners** is a business associate. A business associate may receive protected health information from the medical practice, or it may *create* protected health information for the medical practice.

Protected health information may be disclosed to business associates only if **ProHealth Partners** receives satisfactory assurances that the business associate will safeguard the privacy of the protected health information that it creates or receives **and information security awareness training is provided to all employees (if applicable contractors and third party users) before access is granted to UHG PHI/PII.** Updates in information security policy and procedures shall be given to employees **(if applicable contractors and third party users) annually (at a minimum).** Attestation of training required, see

### **Satisfactory Assurances**

Written contracts or agreements must be negotiated between a medical practice and any business associate that will handle protected health information it receives from or creates for the practice. This contract or agreement must include provisions that:

- Identify the uses and disclosures of protected health information permitted under the contract
- Permit the business associate to use or disclose the information only as permitted under the privacy standards
- Restrict use and disclosure of the protected health information the business associate creates or receives to those that are specified in the contract
- Call on the business associate to establish and use safeguards to prevent use and disclosure other than as provided for in the contract with **ProHealth Partners**, provide for reporting to **ProHealth Partners** any use or disclosure of protected health information not provided for under the business associate's contract
- Require the business associate to apply the same restrictions and conditions on use and disclosure of protected health information to the agents and subcontractors to whom it forwards the protected health information
- Make protected health information available to patients as provided under policy [P-5000](#)
- Amend any protected health information that it receives when asked to do so by **ProHealth Partners**.
- Make available to **ProHealth Partners** the information it needs to account for uses and disclosures of protected health information as provided under [P-7000](#)
- Make internal practices, books, and records related to the use and disclosure of protected health information available to HHS for purposes of determining compliance with the privacy standards
- Return, if feasible, all protected health information to **ProHealth Partners** upon termination of the contract, and destroy any copies of such information. When return and/or destruction of protected health information

is not feasible, the business associate will extend contractual protections to the use and disclosure of the information for the purposes that make its return or destruction not feasible

- Provide for termination of the contract if the business associate violates these contractual provisions

#### **Regulation**

##### **45 CFR 164.504(e)(1) and (2)**

Establishes requirements for contracts with business associates.

#### **P-1410 Duty of Staff to Report Contractual Breaches by Business Associates**

If a staff member becomes aware of activities or practices by the business associate that violate the medical practice's contractual obligations, the activities or practices must be reported to the **Privacy Officer**.

#### **Regulation**

##### **45 CFR 164.504(e)(1)(ii)**

Requires the covered entity to take actions to correct violations of contractual provisions when the covered entity becomes aware of them.

#### **P-1420 Investigation and Correction of Contractual Breaches**

When the **Privacy Officer** is notified that a business associate has violated a contractual provision related to the privacy of protected health information, he or she must implement the following procedure to correct the violation:

In the event there is a breach of PHI, these guidelines/regulations from CMS must be initiated and the Company must be notified immediately by the Business Associate but no later than 30 days after the first date the breach is discovered:

Written notification shall be provided in concise, conspicuous, plain language that includes the following elements:

- A brief description of what happened, including the date(s) of the breach and of its discovery;
- To the extent possible, a description of the types of personal information involved in the breach (e.g., full name, social security number, date of birth, home address, account number, disability code, etc.);
- A statement whether the information was encrypted or protected by other means, when determined such information would be beneficial and would not compromise system security;
- What steps individuals should take to protect themselves from potential harm, if any;
- What Contractor is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches;

and

- Who affected individuals should contact for more information, including a toll-free telephone number, e-mail address, and postal address.

- The **Privacy Officer** will contact the business associate and determine whether a contractual provision has been violated.
- If a contract provision has been violated, the **Privacy Officer** will identify steps to be taken by the business associate that will enable it to comply with its contractual obligations.
- The **Privacy Officer** 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.
- The **Privacy Officer** will monitor the implementation of the corrective action measures by periodically contacting the business associate. The **Privacy Officer** may discontinue monitoring the contract after receiving adequate assurances that the corrective measures have been implemented and that the contract provisions will be complied with in the future.

If it is not possible to develop an acceptable corrective action plan, **the Privacy Officer** should implement the procedures established in policy [P-1430](#) to terminate the contract.

### **Regulation**

#### **45 CFR 164.504(e)(1)(ii)**

Requires the covered entity to take actions to correct violations of contractual provisions when the covered entity becomes aware of them.

### **P-1430 Reporting of Contractual Breaches by Business Associates**

When the **Privacy Officer** is not able correct violations of contractual obligations by a contractor, he or she should implement the following procedure:

- An alternative source for the services provided by the business associate should be identified.
- The matter should be referred to the medical practice’s legal counsel with a request that formal action be taken to terminate the contract.
- The business associate should be notified by the practice’s legal counsel that action will be taken to terminate the contract if the violation of contract provisions is not immediately corrected.
- The status of the contract should be monitored by the **Privacy Officer** and arrangements should be made to replace the business associate when the contract is formally terminated.

If the contract cannot be terminated, the contract violation should be reported by legal counsel to HHS.

### **Regulation**

#### **45 CFR 164.504(e)(1)(ii)(A)**

Requires termination of business associate contracts when it is not possible to end the violation of contractual obligations.

#### **45 CFR 164.504(e)(1)(ii)(B)**

Requires reporting to HHS of contract violations when it is not possible to terminate a business associate contract.

### **P-1500 Development and Maintenance of Privacy Policies and Procedures**

This section of the **ProHealth Partners’** privacy manual:

- Assigns responsibility for developing and updating the privacy manual

- Establishes policies and procedures for updating policies and procedures
- Establishes policies and procedures for obtaining the approval of policies and procedures
- Establishes policies and procedures for communicating updated policies to employees and staff members

### **Regulation**

#### **45 CFR 160.530(i)(1)**

Requires covered entities to establish written policies and procedures to implement the federal privacy standards.

### **P-1510 Responsibility for Developing and Updating the Privacy Manual**

The **Privacy Officer** will develop policies and procedures that are reasonably designed to ensure compliance with federal and state standards for the protection of the privacy of health information. The **Privacy Officer** may delegate this responsibility to a staff member, but such delegation must be reflected in that staff member's job description and the **Privacy Officer** will supervise the development of all privacy policies and procedures.

### **Regulation**

#### **45 CFR 160.530(1)(1)**

Requires covered entities to assign responsibility for development and implementation of policies and procedures to the designated privacy official.

### **P-1520 Procedures for Updating Privacy Policies and Procedures**

It is the responsibility of the **Privacy Officer** to:

- Monitor changes in federal and state law and regulations that may require changes in privacy policies and procedures
- Notify the **ProHealth Partners Board of Directors** of the issuance of new federal or state requirements and describe the need to modify policies and procedures, including the date by which revised policies and procedures must be implemented
- Take the initiative to develop new or revised policies and procedures as necessary to meet the requirements of new laws and regulations
- Identify any revisions that are needed in the privacy orientation and training program to reflect revised policies and procedures

Before a revised policy or procedure is submitted for approval, the **Privacy Officer** will review the Notice of Privacy Practices form (see policy [P-3100](#)) and determine whether the Notice must be revised to reflect the new privacy policies or procedures.

The effective date of a revised policy or procedure must not be earlier than the date on which the revised Notice of Privacy Practices is posted and made available to patients.

### **Regulations**

#### **45 CFR 160.530(i)(1)**

Requires covered entities to implement policies and procedures to comply with the federal privacy standards.

#### **45 CFR 160.530(i)(2)(ii)**

Requires covered entities to update policies and procedures to comply with changes in the law and regulations. Establishes requirements for the effective date of revised policies and procedures.

**45 CFR 160.530(i)(3)**

Requires covered entities to promptly document and implement changes in policies and procedures whenever there is a change in the law requiring such changes

**45 CFR 160.530(i)(4)(i)(C)**

Prohibits implementation of new policies and procedures prior to the effective date of a revised Notice of Privacy Practices, unless an earlier effective date is mandated by law or regulation.

**P-1530 Approval of Policies and Procedures**

All policies and procedures must be approved by the **Board of Directors** of **ProHealth Partners** before they can be implemented.

**P-1540 Communication and Implementation of Revised Policies and Procedures**

New or revised policies and procedures are to be communicated to staff through:

- An all-staff memorandum from the **Privacy Officer** will announce the adoption of the new or revised policies and indicate affected staff functions. This memorandum should describe the new policy, indicate its effective date, and indicate the date on which the new policy will be available for staff review.
- **Privacy Officer** or a designated representative will announce the adoption of the new policies at appropriate staff meetings.
- A targeted memorandum will be circulated by **Privacy Officer** to those staff members whose job responsibilities are directly affected by the new policies. This memorandum should indicate whether training or orientation meetings or programs will be held, and whether background information on the new policy is available. A copy of the revised policy should be attached to the memorandum, or staff should be directed to consult the updated policy and procedure manual.
- The revised policy will be distributed to all staff responsible for maintaining and updating copies of the policy manual that are available to staff.

**Regulation**

**45 CFR 164.530(b)(2)(i)(C)**

Requires training of all workforce members whose job duties are affected by a change in privacy policies and procedures.

**P-1600 Documentation and Record-Keeping**

This section establishes policies and procedures for maintaining records of policy practices and procedures, written notifications, and enforcement actions taken.

**Regulation**

**45 CFR 160.530(j)**

Requires documentation of compliance with privacy rules.

**P-1610 Establishment of Record-Keeping Systems**

The **Privacy Officer** will establish and oversee record-keeping systems to maintain the documentation required in this policy manual.

## **Regulation**

### **45 CFR 160.530(j)(1)**

Requires maintenance of policies and procedures in written or electronic form, retention of written communications, and documentation of required actions, activities, and designations.

## **P-1620 Maintenance of Written Records**

The information to be maintained includes:

- The policies and procedures contained in this policy manual
- The Notice of Privacy Practices
- The signed acknowledgment of receipt of the Notice of Privacy Practices
- Signed authorization forms
- Records of disciplinary actions taken against staff members for violations of privacy policies and procedures
- Records of actions taken to enforce compliance with contract provisions by business associates
- Complaint forms received from patients or other individuals and associated written correspondence
- All requests for an accounting of disclosure of protected health information and records related to such requests
- All requests for amendment of protected health information and records related to the disposition of such requests

## **Regulation**

### **45 CFR 160.530(j)(1)**

Requires documentation of all written communications required by the federal privacy rule, and all actions that the rule requires be documented in writing.

## **P-1630 Retention of Records and Documentation**

All documentation of actions called for by other policies and procedures contained in this manual will be maintained for a minimum of six years from the date the information was created.

In the case of policies and procedures, the six-year retention period will be measured from the date of the most recent revision of the policy. In other words, when new policies are issued, the policies that are superseded should be retained for six years following the last day the policy was in effect.

## **Regulation**

### **45 CFR 160.530(j)(2)**

Requires retention of documentation for six years from the date of creation

## **P-2000 Use and Disclosure of Protected Health Information**

This section of the privacy manual establishes policies and procedures that apply to the use and disclosure of protected health information.

Users should also consult the section of this manual that establishes policies and procedures for providing patients with the Notice of Privacy Practices and obtaining their consent and authorization for uses and disclosure of protected health information.

## **P-2100 Use and Disclosure of Information for Treatment Purposes**

The policies in this section address the use and disclosure of protected health information for the purpose of treatment.

The use and disclosure of information for the purpose of treatment does not require specific authorization (see policy [P-3300](#)). Except in emergency situations, as discussed in policy P-2112, patients must be given the current Notice of Privacy Practices before initiating treatment.

**Regulation**  
**45 CFR 164.506**

Establishes requirements for the use and disclosure of protected health information for the purposes of treatment, payment, and health care operations.

**P-2110 Provision of Notice Prior to Non-emergency Treatment**

Before nonemergency treatment is initiated, an effort must be made to obtain the patient's written acknowledgment of having received the Notice of Privacy Practices. Obtaining the written acknowledgment is the responsibility of the **Front Desk Receptionist**. If the patient's acknowledgment cannot be obtained, the attempt to obtain an acknowledgment should be documented in writing.

Procedures for obtaining the acknowledgment are established by policy [P-3190](#).

**Regulation**  
**45 CFR 164.520(c)**

Requires the Notice of Privacy Practices to be given to the patient prior to treatment.

**P-2120 Sharing Information Outside the Practice**

When a provider who is not a member of the practice contacts a staff member and requests information for the purpose of treating a patient previously treated at **ProHealth Partners**, the staff member may provide information without restriction. It is not necessary for the patient to authorize the disclosure of protected health information that will be used for the purpose of treatment.

When disclosing information to another provider for purposes of payment, staff members should use the following procedure:

- A patient may have requested and been granted restrictions on the use or disclosure of protected health information. Staff members should review the patient's records to determine if any restrictions have been placed on the use or disclosure of protected health information.
- Before disclosing information for treatment purposes, a medical practice staff member must verify the identity of the person making the request. In other words, the staff member must determine that the person making the request is, in fact, a health care professional who is requesting the information for the purpose of treatment. If the professional is known to the practice, is a member of a group that is known to a staff member, or is affiliated with a facility that is known to the practice, a staff member may presume that the provider is who he or she claims to be. Otherwise, a staff member should obtain additional assurances sufficient to satisfy his or her professional judgment that the person requesting the information is a health care provider who will use the information for purposes of treatment.
- Protected health information should be sent only to the verified business address of the provider requesting it.

## **Regulation**

### **45 CFR 164.502(b)(2)**

Exempts disclosure for the purpose of treatment from the *minimum necessary* standard.

### **45 CFR 164.514(h)(1)**

Requires verification of the identify of a person requesting protected health information when the person making the request is unknown to the person receiving the request.

## **P-2130 Requesting Information From Outside the Practice**

When a staff member requires information on a patient's health condition from another provider, he or she may request the information without restriction. The patient need not authorize this request.

The information requested must, however, be used for the purpose of evaluating the patient's medical condition or determining a course of treatment.

A patient may have requested and been granted a restriction on the information that is to be used or disclosed to other providers. In this situation, the restriction must be honored.

## **Regulation**

### **45 CFR 164.514(d)(4)**

Limits requests for protected health information to the minimum necessary for a specified purpose.

## **P-2200 The Use of Patient Information for Payment Purposes**

This section addresses the use and disclosure of protected health information to third-party payers and others for the purpose of obtaining payment for services. These uses and disclosures do not require the patient's specific authorization (see [P-3300](#)).

## **Regulation**

### **45 CFR 164.506(c)**

Permits the use and disclosure of protected health information for the purposes of treatment, payment, and health care operations.

## **P-2210 Definition of Payment Activities**

Use and disclosure of protected health information is permitted under this policy to conduct the following activities:

- Providing information to the patient's health plan to determine the patient's eligibility for benefits and coverage
- Submitting a claim for services to the patient's health plan
- Processing credit card transactions or transactions to obtain authorization for personal checks
- Providing information needed by the patient's health plan to determine coverage, including information needed by the health plan to conduct medical review

Before seeking payment for nonemergency treatment, a patient *must* be given the Notice of Privacy Practices and a written acknowledgment of receipt must be obtained. Obtaining the acknowledgment is the responsibility of the **Front Desk Receptionist**.

Procedures for obtaining an acknowledgment are established by policy P-3190.

**Regulation**  
**45 CFR 164.520(c)**

Requires that the Notice of Privacy Practices be given to the patient prior to treatment.

**P-2212 Application of Minimum Necessary Standard to Payment**

Use and disclosure of protected health information for payment purposes is limited to the information that can be transmitted using the standards for electronic transactions. These restrictions apply whether the transaction is conducted electronically or using paper forms.

**Regulation**  
**45 CFR 164.502(b)(2)(vi)**

Exempts information that is required to comply with the electronic transaction standards from the minimum necessary standard.

**P-2300 The Use and Disclosure of Information for Health Care Operations**

This section addresses the uses and disclosures of information in the course of day-to-day operations that do not require specific authorization (see policy [P-3300](#)).

**Regulation**  
**45 CFR 164.506**

Establishes requirements for the use and disclosure of protected health information for the purposes of treatment, payment, and health care operations

**P-2310 Definition of Health Care Operations**

Use and disclosure of protected health information is permitted under this policy to conduct the following activities:

- Quality assessment and improvement
- Professional credentialing
- Medical and utilization review
- Legal services
- Auditing
- Business planning and market research
- Grievance procedures
- Due diligence analysis related to sales and acquisitions
- Creation of de-identified information and limited data sets
- Customer service
- Patient directories
- Compliance monitoring

Before using or disclosing protected health information for any of the functions included in health care operations, the medical practice must give the patient its Notice of Privacy Practices. Obtaining an acknowledgment of receipt of the notice is the responsibility of the **Front Desk Receptionist**.

Procedures for obtaining an acknowledgment are established by P-3190.

## **P-2400 Law Enforcement and Public Health**

The policies in this section address the disclosure of protected health information to various government entities. In general, disclosure to government entities is mandated by law and does not require the consent or advance authorization of the patient. However, under certain circumstances, the patient must be notified that information has been disclosed.

### **Regulation**

#### **45 CFR 164.512**

Authorizes use and disclosure of protected health information without written consent or authorization for purposes of law enforcement and legally mandated reporting.

## **P-2410 Disclosure of Patient Information to Public Health Agencies**

The following information may be reported to **Department of Health Services** as required by law whether or not the patient consents or authorizes the disclosure:

- Information required to compile vital statistics (births and deaths)
- Information on communicable diseases
- Information on reportable injuries

### **Regulation**

#### **45 CFR 164.512(b)**

Permits disclosure of protected health information to public health authorities when authorized by law.

General Public Health Activities. The Privacy Rule permits covered entities to disclose protected health information, without authorization, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability. This would include, for example, the reporting of a disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions. See 45 CFR 164.512(b)(1)(i). Also, covered entities may, at the direction of a public health authority, disclose protected health information to a foreign government agency that is acting in collaboration with a public health authority. See 45 CFR 164.512(b)(1)(i). Covered entities who are also a public health authority may use, as well as disclose, protected health information for these public health purposes. See 45 CFR 164.512(b)(2).

A “public health authority” is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. See 45 CFR 164.501. Examples of a public health authority include State and local health departments, the Food and Drug Administration (FDA), the Centers for Disease Control and Prevention, and the Occupational Safety and Health Administration (OSHA).

Generally, covered entities are required reasonably to limit the protected health information disclosed for public health purposes to the minimum amount necessary to accomplish the public health purpose. However, covered entities are not required to make a minimum necessary determination for public health disclosures that are made pursuant to an individual's authorization, or for disclosures that are required by other law. See 45 CFR 164.502(b). For disclosures to a public health authority, covered entities may reasonably rely on a minimum necessary determination made by the public health authority in requesting the protected health information. See 45 CFR 164.514(d)(3)(iii)(A). For routine and recurring public health disclosures, covered entities may develop standard protocols, as part of their minimum necessary policies and procedures, that address the types and amount of protected health information that may be disclosed for such purposes. See 45 CFR 164.514(d)(3)(i).

## **P-2420 Reporting of Abuse, Neglect, and Domestic Violence**

Staff may report cases of suspected child abuse or neglect to **State or Local Police Department of Child Abuse and Neglect or County Department of Family Services** as required by law.

Any such reports must follow the policies and procedures that are established in the following policies:

- Policy P-2421 addresses disclosure of protected health information concerning child abuse and neglect that is *required* by law.
- Policy P-2422 addresses disclosure of protected health information concerning abuse, neglect, and domestic violence that is *required* by law. These policies and procedures do not apply to mandated reporting of child abuse and neglect, which is to be handled according to policy P-2421.
- Policy P-2423 addresses disclosure that is permitted but not required by law of protected health information concerning abuse, neglect, and domestic violence.
- Policy P-2424 addresses voluntary disclosure of protected health information concerning abuse, neglect, or domestic violence.
- Policy P-2425 establishes policies and procedures for informing patients of reports of abuse, neglect, or domestic violence.

### **Regulation**

#### **45 CFR 164.512(c)**

Permits disclosure of protected health information to government agencies responsible for investigating abuse, neglect, and domestic violence.

## **P-2421 Mandatory Reporting of Child Abuse and Neglect**

The medical practice must report cases of suspected child abuse or neglect to **State or Local Police Department of Child Abuse and Neglect or County Department of Family Services** as required by law even if the patient does not consent or authorize the disclosure. Staff must limit disclosure only to the types of information that *must* be disclosed. "Child abuse or neglect which must be reported includes:

1. Physical injury inflicted by other than accidental means upon a child by another person
2. Sexual abuse including both sexual assault and sexual exploitation (but pregnancy is not alone sufficient to constitute the basis of a reasonable suspicion of sexual abuse)
3. Willful cruelty or unjustifiable punishment of a child
4. Unlawful corporal punishment or injury (which does not include an amount of force that is reasonable and necessary for a person employed by or engaged in a public school to quell a disturbance threatening physical injury to person or damage to property, for purposes of self-defense, or to obtain possession of weapons or other dangerous objects within the control of the pupil, or otherwise reasonably necessary to

maintain order, protect property, protect the health and safety of pupils, or to maintain proper and appropriate conditions conducive to learning).

5. Neglect, which is defined to mean negligent treatment or maltreatment of a child by a person responsible for the child's welfare where harm to the child's health or welfare is indicated or threatened. Among other things, neglect includes the failure to protect the child from severe malnutrition or medically diagnosed non-organic failure to thrive or any situation in which the person or health of the child is endangered, including failure to provide adequate food, clothing, shelter, medical care, or supervision. An informed and appropriate medical decision made by the child's parent or guardian after consultation with a physician or physicians who have examined the minor does not constitute neglect.

Required reports by telephone and in writing must include:

1. The name, address, and telephone number of the mandated reporter and the capacity that makes the person a mandated reporter
2. The child's name and address, present location, and, where applicable, school, grade and class
3. The names, addresses, and telephone numbers of the child's parents or guardians
4. The information that gave rise to the reasonable suspicion of child abuse or neglect and the source or sources of that information. The mandated reporter may include with the report any non-privileged documentary evidence the mandated reporter possesses relating to the incident
5. The name, address, telephone number and other relevant information about the person(s) who might have abused or neglected the child

## **Regulation**

### **45 CFR 164.512(b)(1)(ii)**

Permits disclosure of protected health information without the patient's consent or authorization that concerns *child abuse and neglect*.

### **45 CFR 164.512(e)(1)**

Permits disclosure of protected health information to government agencies responsible for investigating abuse, neglect, and domestic violence.

## **P-2422 Mandatory Reporting of Abuse, Neglect, and Domestic Violence**

Staff must report cases of suspected abuse, neglect, or domestic violence to **State or Local Police Department** as required by law even if the patient does not consent or authorize the disclosure. Only the types of information that are required by law should be disclosed. This information includes the following:

- Name of the injured person, if known
- The injured person's whereabouts
- The character and extent of the person's injuries
- The identity of any person the injured person alleges inflicted the wound, other injury or assaultive or abusive conduct upon the injured person
- May include; comments by the injured person regarding past domestic violence, or regarding the name of any person suspected of inflicting the injury or engaging in the assaultive or abusive conduct upon the person;
- A map of the injured person's body showing and identifying injuries and bruises at the time of the health care
- A copy of the law enforcement reporting form

The patient must be informed of this report if required under policy P-2425.

## **Regulation**

### **45 CFR 164.512(c)**

Permits disclosure of protected health information to government agencies responsible for investigating abuse, neglect, and domestic violence.

## **P-2423 Non-mandatory Reporting of Abuse, Neglect, and Domestic Violence**

Medical practice staff may report cases of suspected child abuse or neglect to **State or Local Police Department of Child Abuse and Neglect or County Department of Family Services** without the agreement of the patient if the following criteria are met:

- The patient's physician believes that the report may prevent serious injury to the patient or others.
- The disclosure is *permitted* under federal or state law

Medical practice staff should restrict the disclosure to information that can be disclosed legally.

## **Regulation**

### **45 CFR 164.512(c)(1)(iii)**

Permits disclosure of protected health information related to abuse, neglect, and domestic violence when the disclosure is permitted by law and a provider believes it is necessary to prevent harm to the patient or others.

## **P-2424 Voluntary Reporting of Abuse, Neglect, and Domestic Violence with the Patient's Agreement**

Medical practice staff may report cases of suspected child abuse or neglect to **State or Local Police Department of Child Abuse and Neglect or County Department of Family Services** with or without the patient's authorization. Disclosure should be restricted to the types of information that state law or local law allows to be disclosed.

## **Regulation**

### **45 CFR 164.512(c)(1)(ii)**

Permits disclosure of protected health information to government agencies responsible for investigating abuse, neglect, and domestic violence when agreed to by the individual.

## **P-2425 Informing Patients of Disclosures**

The patient must be informed of any disclosure of protected health information to **State or Local Police Department of Child Abuse and Neglect or County Department of Family Services** unless the patient's physician believes that informing the patient may lead to serious harm for the patient or another person or unless state law prohibits such notification.

If it is not possible to inform the patient, the patient's personal representative must be informed of the disclosure unless the patient's physician believes that informing the representative may lead to serious harm for the patient or another person.

## **Regulation**

### **45 CFR 164.512(c)(2)**

Requires notification of a report of abuse, neglect, or domestic violence unless the provider believes that disclosure would put the individual at risk of serious harm.

## **P-2430 Disclosure of Patient Information to Law Enforcement Agencies**

Medical practice staff may disclose the following protected health information requested by law enforcement agencies without obtaining the patient's authorization:

- Medical practice staff members may report certain wounds and physical injuries to **State or Local Law Enforcement Agency** as required by state law. Reportable wounds and injuries include:
- Medical practice staff members may report any information requested by a subpoena, court order, or summons.
- Medical practice staff members may report the name and address, date and place of birth, social security number, ABO blood type and rh factor, type of injury, date and time of treatment or death, and a description of physical characteristics when requested by a law enforcement official. Staff may not report other information such as information related to DNA or DNA analysis, dental records, tissue typing, or the analysis of body fluids or tissues without a court order, subpoena, or summons.
- Medical practice staff members may report protected health information concerning the victim of a crime, but only with the agreement of the victim or when a law enforcement office indicates that the information is needed to investigate suspected criminal activity.
- Medical practice staff members may report protected health information that is evidence of criminal conduct on the premises of the practice.
- Medical practice staff members may report protected health information concerning emergency treatment when the disclosure is necessary to alert law enforcement agencies to the commission of a crime, the location of the victim(s) of a crime, or the identity, description, or location of a suspected perpetrator of a crime.

## **Procedures**

- Medical practice staff members should refer requests for protected health information received from law enforcement agencies to **Privacy Officer**.
- The **Privacy Officer** will review requests for protected health information and obtain a legal opinion if he or she believes one is necessary before approving the disclosure of the requested information.

## **Regulation**

### **45 CFR 164.512(f)**

Permits disclosure of protected health information to law enforcement agencies without authorization

## **P-2440 Disclosure of Patient Information to Oversight Agencies**

Staff may disclose protected health information to government agencies such as the **Department of Health Services**, which are responsible for administering public health programs such as Medicare and Medicaid, and for licensing providers, conducting audits, and other purposes related to the oversight of the health system.

## Procedures

- Staff should refer requests for protected health information received from oversight agencies to **Privacy Officer**.
- The **Privacy Officer** will review requests for protected health information and obtain a legal opinion if he or she believes one is necessary before approving the disclosure of the requested information.

### Regulation

#### 45 CFR 164.512(d)

Permits disclosure of protected health information without consent or authorization to oversight agencies.

## P-2450 Disclosures Related to Judicial and Legal Actions

Medical practice staff members may disclose protected health information for use in a legal proceeding under the following circumstances:

- The information has been requested in a court order or an order of an administrative tribunal.
- The information has been requested by means of a subpoena, discovery request, or other legal process.

Before responding to the request, efforts should be made to ensure that disclosure is limited to the minimum protected health information specifically requested, and that the following assurances are obtained:

- The party seeking the protected health information has made a good faith effort to provide a written notice to the subject of the request, has provided sufficient information to the subject of the request to permit the individual to object to the disclosure, and has resolved any objections that may have been raised.
- The party seeking the protected health information provides written documentation that it has entered into or otherwise obtained a qualified protective order that (a) prevents the parties to the legal action from using or disclosing protected health information for any purpose not related to the litigation or legal proceeding for which the information was requested, and (b) requires the return or destruction of the protected health information at the conclusion of that proceeding.

## Procedures

- Unless a request is referred by the **Privacy Officer**, medical practice staff members should refer requests for protected health information from law enforcement agencies to **Privacy Officer**.
- The **Privacy Officer** will notify and seek guidance from legal counsel on how to respond to the request.
- Before responding, the **Privacy Officer** will obtain the assurances described in this policy.

### Regulation

#### 45 CFR 164.512(e)

Permits disclosure of information for judicial and administrative proceedings, subject to specific requirements and assurances.

## P-2500 Marketing and Fundraising

This section addresses the use of protected health information in marketing and fundraising activities. Whether the patient's authorization is required for fundraising and marketing depends on how marketing communications and fundraising appeals are structured by the medical practice.

### P-2510 Marketing Communications That Require Authorization

The following types of communications do not require authorization:

- Communications to members of health plans that describe the medical practice, its members, and the services that are available from the practice
- Communications to a patient as part of the patient's treatment that are specific to the medical condition of the patient
- Communications from the patient's health plan during treatment for the purpose of alerting the patient to the availability of alternative treatments, therapies, health care providers, or treatment settings
- Face-to-face communications between medical practice staff members and patients during a patient visit
- Promotional gifts of nominal value such as pens, note pads, or coffee mugs

### **Regulation**

#### **45 CFR 164.501**

The definition of marketing specifically excludes communications describing "a health-related product or service...that is provided by...the covered entity making the communication" and communications that are for the treatment of the individual.

### **P-2520 Marketing Activities That Require Authorization**

Most uses and disclosures for marketing purposes, including subsidized treatment communications, will require the individual's authorization.

Most disclosures of PHI that constitute the sale of PHI will require the individual's authorization. Other uses and disclosures not described in the NPP will be made only with authorization from the individual.

Patients must specifically authorize the use of protected health information collected or maintained by the medical practice for a communication that is sent to the individual describing a product or service offered by an organization other than the medical practice. Examples include mailings by pharmaceutical companies, retail pharmacies, health clubs and suppliers of unrelated medical services such as durable medical equipment.

### **Regulation**

#### **45 CFR 164.514(e)(1)**

Requires authorization for use of protected health information in marketing

### **P-2530 Fundraising Activities**

The patient may be contacted for fundraising purposes; however, the individual has the right to opt out of such fundraising communications with each solicitation.

The following information may be used to support efforts to raise funds that directly benefit the medical practice without obtaining the patient's authorization:

Demographic information describing the individual (i.e., date of birth, sex, marital status, address, and other non-clinical information that describes the patient)

The dates on which the patient received health care services from the medical practice

Other protected health information may not be used in fundraising activities without authorization by the patient. That is, the patient's authorization is required for the use of any protected health information except demographic information and dates of service.

Fundraising appeals sent to individuals must include the following paragraph describing how the individual may opt-out of further fund-raising communications:

To be removed from future fundraising appeals, please call **(562) 491-9274** and ask to be removed from our fundraising mailing list, or check off the box asking to be removed from our fundraising mailing list on the reply card and return it to the office by dropping it in a mailbox.

A fundraising mailing list will be maintained by **ProHealth Partners**. When a patient asks to be removed from the mailing list, a reasonable effort will be made to accommodate this request.

Protected health information may not be used to support fundraising on behalf of other organizations (that is, for raising funds that do not benefit the practice directly) without the patient's authorization.

### **Regulation**

#### **45 CFR 164.514(f)(1)**

Permits use and disclosure of protected health information for fundraising purposes only with the patient's authorization.

## **P-2600 Other Disclosure Situations**

### **P-2610 Disclosure of Information for the Purpose of Cadaveric Organ Donation**

Following the death of a patient, a medical practice may disclose protected health information to an organ procurement organization such as an eye bank or tissue bank without the patient's prior authorization, and without obtaining the authorization of the patient's representative.

Medical practice staff members may *not* disclose this information if a patient or the patient's representative has indicated that he or she does not want to donate organs or tissue, or if the patient has imposed a restriction on the disclosure of protected health information for this purpose.

### **Regulation**

#### **45 CFR 164.512(h)**

Permits use and disclosure of protected health information without authorization by the patient to facilitate organ donation and transplantation.

### **P-2620 Disclosure of Information to Coroners and Medical Examiners**

Medical practice staff members may disclose protected health information without the patient's authorization to a coroner or medical examiner who requests the information for the following purposes:

- Identification of a deceased person
- Determination of the cause of death
- Other purposes specified in state or federal law

### **Procedures**

- The credentials of the coroner or medical examiner making the request should be verified. If the request is made in person, staff should ask to be shown an official identification. If the request is made by telephone, staff should ask that the request be submitted in writing and should obtain the official address to which information should be sent.
- Medical practice staff members should confirm that the information is being requested by the coroner or medical examiner for use in establishing the identify of a deceased person or determining the cause of death.

- The requested information should only be sent to the official address of the coroner or medical examiner.

### **Regulation**

#### **45 CFR 164.512(g)(1)**

Permits disclosure of protected health information to a coroner or medical examiner for purposes specified in federal or state law.

### **P-2630 Disclosure of Information to Funeral Directors**

A medical practice may disclose protected health information requested by a funeral director for the purpose of preparing a body for burial or cremation.

Medical practice staff members should attempt to obtain the permission of the patient or patient's representative before disclosing requested information, but permission is not required.

Only the information that a funeral director is entitled to request under state laws should be disclosed.

### **Procedures**

- The funeral director should be asked to submit a written request for the required information. This request may be faxed, but should identify the funeral director by name and address.
- An attempt should be made to contact the patient's representative or a close family member (spouse, child, or other family member) or close personal friend who has been involved in the patient's treatment for permission to disclose the requested information.
- The requested information should only be sent to the business address of the funeral director.

### **Regulation**

#### **45 CFR 164.512(g)(2)**

Permits disclosure of protected health information to funeral directors when consistent with federal or state law.

### **P-2640 Disclosure to Avert a Threat to Health or Safety**

A medical staff member may disclose the following protected health information without the consent or authorization of the patient if, in his or her professional judgment, such disclosure is necessary to reduce a serious and imminent threat to the health and safety of a person or the public:

- Information may be disclosed *only* to a person who is able, in the judgment of the staff member, to prevent or lessen the threat.
- If the patient has threatened to harm or injure another person or persons, that threat may be disclosed to the person(s) identified by the patient as the target(s).
- If the patient has admitted that he or she has participated in a violent crime, that admission may be disclosed to law enforcement agencies.
- If the staff member has reason to believe, based on all circumstances, that the patient has escaped from a correctional facility or lawful custody, the staff member may disclose that belief to law enforcement agencies.

Medical staff members may *not* disclose information related to participation in a violent crime if that information is learned in the course of treatment, counseling, or therapy for a propensity to engage in the criminal conduct, or if the patient has disclosed criminal activity while requesting referral for treatment, counseling, or therapy of such a propensity.

## **Regulation**

### **45 CFR 164.512(j)**

Permits disclosure of protected health information to avert a threat to health or safety.

## **P-2650 Disclosure to Disaster Relief Agencies**

Information on a patient's location, medical condition, or death may be disclosed to disaster relief organizations such as the Red Cross and other public or private organizations.

## **Regulation**

### **45 CFR 164.510(b)(4)**

Permits use or disclosure of protected health information to assist with disaster relief efforts by a public or private entity.

## **P-2700 Disclosure of Protected Health Information After Death**

The protected health information of a deceased individual will be handled according to the policies and procedures applied to the protected health information of living patients. The death of a patient does not reduce the privacy protections that his or her protected health information will receive.

## **Regulation**

### **45 CFR 164.502(f)**

Requires covered entities to continue to apply all standards for use and disclosure of protected health information to the records of a deceased individual.

## **P-3000 Notice and Authorization**

The policies in this section establish procedures for developing the Notice of Privacy Practices form and obtaining patient authorization for use and disclosure of protected health information.

## **Regulation**

### **45 CFR 164.508**

Establishes requirements for authorization of uses and disclosure that are not covered by the notice.

### **45 CFR 164.520**

Establishes requirements for the Notice of Privacy Practices.

## **P-3100 Notice of Privacy Practices**

The **Privacy Officer** is responsible for developing the Notice of Privacy Practices.

The Notice of Privacy Practices must be written in language that most patients of average intelligence and education will be able to understand.

The notice must contain the elements discussed below.

The following language must appear exactly as it is shown here and must be prominently displayed at the top of the notice.

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

**Uses and Disclosures**

This section of the notice must describe and give examples of the uses and disclosures for purposes of treatment, payment, and health care operations covered by the notice.

It must identify the legally mandated disclosures that may be made without the patient's authorization.

It must indicate that any other use or disclosure of protected health information requires written authorization by the patient, and that an authorization may be revoked by the patient.

**Additional Uses of Information**

The uses and disclosures listed in this section must be specified if the medical practice intends to use protected health information for any of the listed activities. This section can be merged with the previous section.

This section identifies any use of protected health information in the preparation of appointment reminders, in offering information about treatment and other health-related benefits or services, or to conduct fundraising for the practice.

**Note**

An additional use or disclosure that the privacy rule requires concerns disclosure of information to plan sponsors. This information is, however, relevant only to disclosures by a health insurance issuer (including an HMO) to a group health plan. If, however, a practice is preparing a notice for use by a health plan that it sponsors, this use or disclosure should be listed.

**Individual Rights**

This section of the Notice of Privacy Practices must identify the rights of the patient under the federal privacy rule. These must include:

- The right to request restrictions
- The right to receive confidential communications
- The right to inspect and copy protected health information
- The right to amend protected health information
- The right to receive an accounting of disclosures
- The right to receive notification of any breach of his/her unsecured PHI
- The right to request restrictions on PHI disclosures to the individual's health plan for health services or items paid out-of-pocket in full.
- The right to opt out of fundraising communications
- The right to authorize disclosures of psychotherapy notes
- The right to receive a printed copy of the Notice of Privacy Practices itself

**ProHealth Partners Duties**

This section describes the duties of the medical practice, specifically with respect to maintaining the privacy of protected health information, giving the Notice of Privacy Practices to patients, and abiding by the terms of that notice.

**Right to Revise Privacy Practices**

The notice must clearly state that the medical practice reserves the right to modify its privacy practices and that should it do so, the revised notice will be made available to patients upon their request.

## **Complaints**

This section must outline the procedure for submitting complaints concerning the medical practice's privacy practices, or to report suspected violations of privacy rights.

It also must indicate that the medical practice will not retaliate against the patient for submitting a complaint or reporting a suspected violation.

## **Contact Person**

This section of the must give the name, address, and telephone number of the privacy contact designated in policy [P-1100](#).

## **Effective Date**

This section must give the effective date of the Notice of Privacy Practices.

The effective date may not be earlier than the date on which the notice is printed and made available for distribution.

In the case of revisions to the notice, the effective date of the revised notice may not be earlier than the printing and release date of the revised notice. In other words, the policies described in the notice cannot go into effect before patients have been informed of the policies.

### **Regulation**

#### **45 CFR 164.520(b)**

Specifies the required content of the notice.

## **P-3120 Providing the Notice of Privacy Practices to Patients**

The Notice of Privacy Practices will be made available to all patients.

### **Procedure**

- All patients will be given a copy of the notice during their first contact following March 31, 2003, whether in-person in the office, via a telephone consultation, or through other electronic means such as e-mail.
- Any patient who requests a copy of the notice will be given a copy.
- A copy of the notice will be posted in waiting areas.
- If the practice maintains a Web site, the notice will be posted on the practice's Web site.

An individual who receives a copy of the notice electronically (by e-mail) also may request a printed copy of the notice.

### **Regulation**

#### **45 CFR 164.520(c)(2)**

Establishes requirements for providing the Notice of Privacy Practices to patients.

#### **45 CFR 164.520(c)(3)**

Establishes requirements for making the Notice of Privacy Practices available electronically to patients.

## **P-3190 Acknowledgment of the Notice**

All patients must be asked to sign an acknowledgment that they have received a copy of the Notice of Privacy Practices.

If the patient cannot sign the acknowledgment, his or her personal representative may sign the acknowledgment.

If the patient cannot sign the acknowledgment and a personal representative is not available, or if the patient refuses to sign the acknowledgment, the staff member who requests the acknowledgment must document the attempt to obtain an acknowledgment and briefly summarize the reason it was not obtained.

When a patient requires emergency treatment, providing the notice and obtaining an acknowledgment should be delayed until the patient's condition has been stabilized.

Copies of all signed acknowledgments should be included in the patient's medical record or filed with the **Privacy Officer**.

**Regulation**

**45 CFR 164.520(c)(2)**

Requires providers to provide the notice and make a good faith effort to obtain the patient's acknowledgment of receiving the notice.

**Regulation**

**45 CFR 164.502(g)(1)**

Allows a personal representative of a patient to act on behalf of the patient.

**P-3300 Authorization of Use or Disclosure**

In HIPAA's language, "authorization" refers to permission to use or disclose protected health information for a specific purpose other than the treatment of the patient, obtaining payment, or for the operation of the practice.

- "Use" refers to the use of the information by a member of the staff of the practice.
- "Disclosure" refers to the disclosure of information to a person or organization separate from the medical practice.

Examples of uses and disclosures for which authorization would be required include:

- Providing camp physicals or medical examinations required for participation in athletic activities
- Providing mailing lists to other organizations (e.g., pharmaceutical companies, charities, etc.) for marketing campaigns
- Participating in medical research and clinical trials

**Regulation**

**45 CFR 164.508**

Establishes requirements for authorization.

**P-3310 Elements of a Valid Authorization**

The authorization obtained from a patient must be written in plain language. The authorization must include the elements discussed below.

### **Information to Be Used or Disclosed**

This section must list the information that will be used or disclosed to others. The description should specify the nature of the information covered by the authorization. The medical practice should not rely instead on a blanket statement that covers any and all information that may be collected or received by the practice.

### **Persons Authorized to Use or Disclose Information**

This section must identify specific medical practice staff who will use or disclose the information. The authorization may specify a class of staff members who are authorized to use or disclose the information (e.g., the members of an identifiable research team).

### **Persons to Whom Information May Be Disclosed**

This section must specifically identify the person or persons to whom the information will be disclosed. The authorization may designate a class of individuals such as the principal investigator of a research project at a specific university.

### **Purpose of Requested Use or Disclosure**

This section must describe the purposes for which the information will be used or disclosed. When an individual initiates the authorization (e.g., for a school or camp physical) this section may simply state “at the request of the individual.”

### **Expiration Date of Authorization**

This section must specify a date after which the information described in the first section may no longer be used or disclosed. When information is to be used for research, the expiration section may simply state “none” or “end of the research study.”

### **Right to Terminate or Revoke Authorization**

This section must specifically describe the right of the patient to revoke the authorization, any restrictions on the ability of the patient to revoke the authorization, and the procedures for revoking the authorization.

### **Potential for Re-disclosure**

This section must include a statement explaining that information used or disclosed under the authorization may be re-disclosed by the individual or organization receiving it and that re-disclosed information may not be protected by the federal privacy rules.

### **Impact on Treatment**

This section must clearly describe the effect of refusing to authorize the requested use and disclosure of protected health information.

If the authorization is not for research-related treatment, a statement must appear explaining that the patient may not be denied treatment if he or she does not authorize the requested use and disclosure of protected health information.

If the authorization is for research-related treatment, a statement may be included indicating that authorization is required to receive the research-related services. This statement is not, however, required unless authorizing use or disclosure is a precondition for receiving treatment.

### **Remuneration**

This section must describe whether the use or disclosure will result in remuneration, directly or indirectly, for the medical practice or a staff member. This section is required only for authorization of uses and disclosures related to marketing. It is not required for research-related authorizations.

### **Signature**

The patient or a personal representative must sign and date the authorization. If a personal representative signs the authorization, he or she must describe the source of their authority to sign on the patient's behalf. Legal power of attorney is one such source of authority.

### **Regulation**

#### **45 CFR 164.508(c)**

Establishes the core elements that must be present in all authorizations.

### **P-3320 Obtaining Authorization for Use or Disclosure**

When a medical practice staff member knows in advance of collecting or creating protected health information that the information will be used or disclosed for a purpose not covered by the notice, the staff member should seek the patient's authorization at that time it is collected.

It is not necessary, however, to obtain the patient's authorization before the information is created. Authorization can be obtained at any time after it is created but before the information is used or disclosed for a purpose not covered by the notice.

The medical practice staff member who uses or discloses the information is responsible for obtaining the patient's authorization.

The patient or patient's representative must be given a copy of the signed authorization.

### **Procedures**

- The medical practice staff member requesting the authorization should obtain an authorization form and complete the sections describing the information to be used or disclosed, the purposes of the use or disclosure, the persons who will use or disclose the information, and the persons to whom the information will be disclosed. See policy P-3310 for required elements.
- The medical practice staff member or a person designated by the staff member should review the authorization request with the patient.
- The patient may request restrictions on the use and disclosure of protected health information. The medical practice staff member requesting the authorization should consider these requests and may, at his or her discretion, accept or reject them. Accepted restrictions should be clearly noted on the authorization form.
- The patient should sign and date the authorization form.

- The signed and dated authorization form should be placed in the patient's record.
- The patient must be given a copy of the signed and dated authorization form.

### **Regulation**

#### **45 CFR 164.508**

Establishes procedures for authorizing uses and disclosures of protected health information.

### **P-3330 Patients' Refusal to Sign an Authorization Form**

A patient who refuses to authorize a specific use or disclosure may not be refused treatment except under the following circumstances:

- The treatment is available only to participants in a research study. A patient who does not authorize use of information for research may be refused treatment that is available only to participants in the research study.
- The services to be provided have no purpose other than responding to a request for information from another entity (for example, from a parent requesting a physical for a child who wants to participate in sports programs).

### **Procedure**

- When a patient refuses to sign an authorization, it should be determined whether the request involves information included in either of the two categories listed above.
- If the authorization is for use and disclosure of information for purposes of research-related treatment, the patient should be told that the treatment is available only to participants in a study, and that participants must authorize use and disclosure of their information in the study.
- If the authorization involves a request for information from another organization, the patient should be told that the services will not be provided unless disclosure is authorized.
- If the patient continues to refuse to sign the authorization, the persons requiring the authorization should be notified of the patient's refusal.

### **Regulation**

#### **45 CFR 164.508(b)**

Prohibits conditioning of treatment on the patient's agreement to authorize use and disclosure of protected health information with the exception of research-related treatment.

A medical practice may require an authorization before providing health care services that have no purpose other than responding to a request for information by another entity.

### **P-3340 Revoking Authorization for Use or Disclosure**

**A patient may revoke an authorization. The revocation must be in writing and must be attached to the related authorization.**

### **Procedure**

- A patient who indicates that he or she wants to revoke an authorization should be given an authorization revocation form.
- The medical practice staff member who sought the original authorization, if he or she is available, or another staff member should explain to the patient that revoking the authorization will not affect any use or disclosure of information that has already occurred.

- The patient should sign and date the revocation form.
- The revocation form should be appended and attached to the authorization and included in the patient's records.

## **Regulation**

### **45 CFR 164.58**

Establishes requirements for revocation of authorization.

## **P-3400 Patient Requests for Restrictions on Uses and Disclosures and Confidential Communications**

Patients may request two types of privacy protections:

- Policy P-3410 addresses restrictions on the use and disclosure of protected health information as provided for by either the consent or an authorization.
- Policy P-3420 addresses confidential communications.

## **Regulation**

### **45 CFR 164.522(a)**

Enables patients to request restrictions on the use and disclosure of protected health information for treatment, payment, and health care operations.

### **45 CFR 164.522(b)**

Enables patients to request confidential communications.

## **P-3410 Patient Requests for Restrictions on Use and Disclosure**

A patient may request restrictions on the use and disclosure of protected health information for treatment, payment, and health care operations as provided for in the standard consent form. A patient also may request restrictions on the use and disclosure of protected health information covered by an authorization form.

The medical practice should consider these patient requests, but is not required to accept them. The practice will generally accept a request for a restriction on the uses and disclosures that are permitted under the standard consent or authorization only if the following criteria are met:

- The request will not impede treatment, payment, or day-to-day functioning of the practice.
- The restrictions will not interfere with the purpose for which an authorization is being sought.
- The patient has valid reasons for requesting the restrictions, in the judgment of the patient's physician.

Once the medical practice accepts requested restrictions, they must be honored unless doing so would interfere with emergency treatment.

All restrictions to which the practice agrees must be documented on the authorization or consent form.

A restriction on the disclosure of information that a patient requests and that the practice agrees to does not prevent the practice from disclosing information that is mandated by law and that does not ever require the patient's consent or authorization.

## Procedure

- A patient may request a restriction on the use or disclosure of information at the time he or she signs a consent or authorization form.
- The request should be reviewed by **Privacy Officer** or by a staff member designated by the **Privacy Officer** to determine whether the requested restriction would impede the use of information for treatment, payment, or health care operations.
- The **Privacy Officer**, or the designated staff member should ask the patient to explain why he or she is seeking the restriction.
- The restriction should be agreed to if, in the judgment of the **Privacy Officer**, it will meet the requirements set out in this policy.
- If the request is agreed to, it should be documented on the consent or authorization form to which it applies.

## Regulations

### 45 CFR 164.522(a)(1)

Enables patients to request restrictions on the use and disclosure of protected health information for treatment, payment, and health care operations.

### 45 CFR 164.522(a)(3)

Requires documentation of restrictions on use and disclosure of protected health information to which the provider agrees.

## P-3411 Termination of Restrictions On Use and Disclosure

The practice may terminate a restriction on the use and disclosure of protected health information to which it has agreed.

Patients must be notified of any termination of a restriction and must be given an opportunity to agree or disagree with the termination.

- If the patient agrees to the termination, information collected prior to the date of the termination may be used or disclosed as though the restriction had never been accepted.
- If the patient does not agree to the termination, only information collected after the date of the termination may be used or disclosed without considering the restriction. The restriction will continue to apply to information collected prior to the date of the termination.

The termination of a restriction must be attached to the consent form or authorization form in which the restriction appears.

## Procedure

- A staff member who wishes to terminate a restriction should contact **Privacy Officer** and discuss the need for the termination.
- The termination request should be approved if the continuation of the restriction would substantially impede treatment, payment, or the day-to-day operation of the practice.
- The staff member should contact the patient to discuss the need for the termination and to seek his or her agreement.
- If the patient agrees to end the restriction, he or she should sign a statement to that effect. If the patient is not available to sign a written statement, his or her oral agreement should be noted, signed, and dated by the staff member who discussed the termination with the patient.

- The termination of the restriction should be attached to the consent or authorization form in which the restriction appears.

## Regulation

### 45 CFR 164.522(a)(2)

Permits termination of a restriction to which a provider has agreed when the patient agrees to terminate the restriction either orally or in writing.

## P-3420 Patient Requests for Confidential Communication

Staff members must accommodate a patient's request for confidential communication if the following criteria are met:

- The patient provides an alternative address or telephone number at which he or she may be contacted.
- The request can be accommodated without limiting the ability of the medical practice to submit claims to the patient's health plan.

If the request for confidential communication will prevent the practice from submitting claims to the patient's health plan, the request will be accommodated only if the patient identifies another method of paying for services provided by the medical practice.

**The patient may restrict PHI disclosures to the individual's health plan for health services or items paid out-of-pocket in full. Form PF-8000**

Requests for restriction must be made in writing using Form PF-8000. The staff member may provide the patient with a **Form PF-8000 Request For Restriction On Use/Disclosure of PHI** or the patient may simply submit a written request.

The staff member may not require the patient to explain why he or she wants to receive confidential communications, although the staff member is permitted to request such an explanation. The patient may refuse to provide any explanation or justification for his or her request.

## Procedure

- When a patient requests confidential communication of protected health information (for example, the results of diagnostic tests), the staff member to whom the request is made should tell the patient that the request must be made in writing and explain the conditions that must be met before the request will be granted (paid out-of-pocket in full).
- The patient should be given a **Form PF-8000 Request For Restriction On Use/Disclosure of PHI** by the staff member to whom the request is made or by a staff member he or she identifies.
- If the medical record is electronic the restricted information should be placed in a secure field in the data file. If the medical record is a paper chart, the restricted information should be placed in a secure area of the chart and marked "Restricted, not to be disclosed without patient authorization".
- The request for confidential communication should be documented on the patient's consent form.

## Regulation

### 45 CFR 164.522(b)

Requires providers to accommodate reasonable requests by patients for confidential communication of protected health information.

## **P-4000 Personal Representatives, Parents, Spouses and Others**

The policies in this manual section establish policies and procedures for:

- Allowing a personal representative to act in the place of a patient for purposes of consenting to the use and disclosure of protected health information
- Disclosing protected health information about a patient to the patient's personal representative(s)
- Disclosing protected health information to the parents or legal guardians of un-emancipated minors
- Disclosing protected health information to family members and close personal friends of adult patients

The goal of these policies is to enable staff members to share protected health information, with the permission of the patient, with those people who are involved in the patient's care, or who are legally responsible for the patient's care.

### **Regulation**

#### **45 CFR 164.508(g)**

Establishes standards that enable a personal representative to act on behalf of a patient.

## **P-4100 Personal Representatives**

A personal representative may act on behalf of the patient for the purpose of:

- Authorizing use and disclosure of protected health information
- Receiving information that otherwise would be sent to the patient

### **Regulation**

#### **45 CFR 164.502(g)(1)**

Allows a personal representative to act on behalf of the patient for purposes of consenting and authorizing use and disclosure of protected health information.

## **P-4110 Designation of a Personal Representative**

A personal representative may be the spouse, adult child, or other member of the patient's family. A personal representative also may be a close personal friend, or any individual with power of attorney or other legally recognized authority to make medical decisions on behalf of the patient if he or she is incapacitated or otherwise unable to make decisions.

A patient may designate a personal representative in writing. However, a person who is identified in the patient record as having medical power of attorney or other legal authority to act on behalf of the patient will be recognized as a personal representative.

A parent or legal guardian of an unemancipated minor (generally a child under the age of 18) will be recognized as a personal representative of the child.

### **Procedure**

- The **Front Desk Receptionist** should ask the patient to identify an individual or individuals who may act as the patient's personal representative on the acknowledgment form.
- If a patient becomes incapacitated, a person accompanying the patient will be recognized as the patient's personal representative if he or she can present evidence of having legal power of attorney or other legally recognized authority to make medical decisions on behalf of the patient.

- The parent or legal guardian of an unemancipated minor will be recognized as the personal representative of a child, subject to the restrictions contained in policy P-4200.

#### **Regulation**

##### **45 CFR 164.502(g)(2)**

Defines the personal representative of an adult or emancipated minor as a person who legally has authority to make health care decisions on behalf of the individual.

#### **P-4120 Authority of Personal Representative**

If a patient is incapacitated, a personal representative may sign any form (such as authorization, revocation of authorization, and request for access to information), the uses of which are described in this privacy manual.

A personal representative may receive protected health information concerning the patient necessary to carry out the representative's legal duties to the patient (for example, providing an informed consent to treatment, or for enforcing an advance directive concerning life support).

Policy [P-4130](#) defines the information that may be disclosed to a personal representative.

#### **Regulation**

##### **45 CFR 164.502(g)(2), (3), and (4)**

Defines the authority of personal representatives to act on behalf of a patient or to receive information on his or her behalf.

#### **P-4130 Refusal to Recognize Personal Representative**

A medical practice staff member may refuse to disclose information to a person identified as a patient's personal representative if the staff member believes that disclosing such information may endanger the patient.

#### **Procedures**

- A medical practice staff member who believes that disclosing information to a personal representative may endanger the patient should notify the **Privacy Officer**.
- Requests from the personal representative for information concerning the patient should be referred to the **Privacy Officer**.

#### **Regulation**

##### **45 CFR 164.502(g)(5)**

Permits the provider to refuse to recognize a personal representative when there is a reasonable basis to believe that doing so would endanger the patient.

#### **P-4200 Parental Access to Protected Health Information Concerning Children**

A parent, guardian or other person recognized by state law as acting *in loco parentis* on behalf of a patient who is an unemancipated minor will be recognized as the patient's personal representative. Note: In this policy the term *parent* refers to a parent, guardian, or other person acting *in loco parentis*.

A parent may act as a personal representative unless state or other law permits the minor to request that information not be shared with a parent, guardian or other person acting *in loco parentis*.

Generally, the medical practice will require a parent or legal guardian's signature on any authorization forms for a minor patient unless the patient requests that his or her parents not be notified.

## **Procedure**

- The **Privacy Officer** should review any minor's request for confidentiality pertaining to the use or disclosure of protected health information that relates to a parent or guardian, to determine whether the request complies with state and federal laws.

### **Regulation**

#### **45 CFR 164.502(g)(3)**

Authorizes parents to act as the personal representatives of unemancipated minors and establishes exceptions to that authority.

## **P-4300 Disclosure of Information to Family Members and Relatives**

Protected health information concerning a patient may be disclosed to a family member, other relative, or close personal friend of the individual who requires the information to assist in the patient's care and treatment.

If the patient is able to, he or she must agree to the sharing of this information before it occurs. Patients should generally be asked whether information may be shared with family members. However, permission can be assumed if the patient has an opportunity to object to disclosure of information to family members and does not do so.

If the patient is incapacitated, a medical practice's staff members may exercise their professional judgment in determining when it is in the patient's best interests to disclose protected health information to the family member.

The information that may be disclosed to a family member, relative or close personal friend is limited to information directly relevant to the family member's involvement in the patient's care.

## **Procedure**

- If possible, disclosure of information to others should occur when the patient is present, or after the patient has agreed to the disclosure.
- If the patient is present or available for consultation concerning the disclosure, he or she should be given an opportunity to object to the disclosure. If the patient objects to the disclosure, the information should not be disclosed.
- If the patient is not present or available for consultation, or is incapable of agreeing or objecting to the disclosure, the attending physician should exercise his or her best professional judgment to determine whether disclosure is in the best interest of the patient.
- If the patient agrees to the disclosure or the disclosure is determined to be in the best interest of the patient, only that information that is directly relevant to the family member's involvement in the patient's care should be disclosed.

### **Regulation**

#### **45 CFR 164.502(g)(2)**

Defines the personal representative of an adult or emancipated minor as a person who legally has authority to make health care decisions on behalf of an individual.

#### **45 CFR 164.510(b)(1)(i)**

Permits disclosure to a family member of protected health information that is relevant to the involvement of that family member in the patient's care.

## **P-4400 Disclosure of Information to Close Personal Friends**

A patient's protected health information may be disclosed to a close personal friend of the patient who requires this information to assist in the patient's care and treatment.

The policies and restrictions found in policy [P-4300](#) should also be applied to disclosures to close personal friends who are directly involved in the patient's care.

### **Regulations**

#### **45 CFR 164.502(g)(2)**

Defines the personal representative of an adult or emancipated minor as a person who legally has authority to make health care decisions on behalf of an individual.

#### **45 CFR 164.510(b)(1)(i)**

Permits disclosure of relevant protected health information to a close personal friend of the patient.

Allows use of protected health information to notify a close personal friend of a patient's location, general condition, or death.

## **P-5000 Patient Access to Health Information**

This section of the privacy manual addresses a patient's request to inspect, copy, or amend his or her protected health information maintained by **ProHealth Partners**.

Policies [P-5100](#) through [P-5140](#) establish procedures for handling patient requests to inspect or copy personal health information.

Policies [P-5200](#) through [P-5242](#) establish procedures for handling patient requests to amend personal health information.

### **Regulations**

#### **45 CFR 164.524**

Requires procedures for patient inspection and copying of protected health information.

#### **45 CFR 164.526**

Requires procedures for patient requests to amend protected health information.

## **P-5100 Patient Requests for Access to Protected Health Information**

A patient or a patient's representative may, subject to approval under policy [P-5120](#), inspect and obtain a copy of his or her information maintained in medical records or other information systems of **ProHealth Partners**.

### **Procedures**

- A patient must submit a request to inspect or copy protected health information as provided for in policy [P-5110](#).
- The request will be reviewed under policy [P-5120](#).
- If the request is denied, the patient will be informed as provided for in policies [P-5130](#) to [P-5132](#).

- If the request is approved, the patient will be given access to the requested information as provided under policies P-5140 to P-5143.

## **Regulations**

### **45 CFR 164.524(1)**

Requires medical practices to allow patients to inspect and copy protected health information, subject to certain restrictions.

## **P-5110 Request for Access to Protected Health Information**

A patient must request in writing an opportunity to inspect or copy his or her protected health information.

This policy does not address or prevent a physician from sharing the results of laboratory or other diagnostic tests with a patient or a patient's personal representative, or from discussing the results of medical procedures. These communications related to treatment may be made orally or in writing at the discretion of the patient's physician.

This policy does not address or prevent other staff members from discussing or disclosing to the patient, orally or in writing, information related to the current status of claims that have been submitted to the patient's health plan.

## **Procedures**

- When a patient or patient's representative requests access to information, he or she should be told that all requests to inspect or copy protected health information must be submitted in writing. The patient should be referred to **Privacy Officer**.
- The **Privacy Officer** will give the patient or patient's representative a copy of a request form and explain the medical practice's policies on allowing patients to inspect their information.
- Upon receipt of a request form, the **Privacy Officer** will forward the request to **Privacy Officer** to be reviewed as explained in policy P-5120.

## **Regulation**

### **45 CFR 164.520(c)(iv)(C)**

Requires the Notice of Privacy Practices to include the right to inspect protected health information.

### **45 CFR 164.524(b)(1)**

Permits providers to require written requests for access to protected health information.

## **P-5120 Review of Patient Requests for Access to Protected Health Information**

The request for access to personal health information will be sent promptly to **Privacy Officer**. A copy of the request will be filed in the patient's records.

The **Privacy Officer** will consider the restrictions on access listed below when determining whether to approve or deny the request to inspect or copy protected health information.

A decision to grant the patient or patient's personal representative permission to inspect or copy the requested information will be made within 30 days of the date on which the request is submitted.

## Restrictions on Access

- Psychotherapy notes will not be made available to the patient unless approved by the treating therapist or successor.
- Information compiled in anticipation of, or for use in, legal proceedings will not be made available to the patient or patient's legal representative unless required by law or court order.
- Information that, by law, may not be disclosed to the patient will not be made available to the patient or patient's representative.
- Information will not be made available if the patient's physician believes that it is likely to endanger the life or physical safety *of the patient*.
- Information will not be made available if the patient's physician believes that access to the information is reasonably likely to cause substantial harm *to a person other than the patient* who is referenced in the patient's records.
- Information will not be made available to a personal representative of the patient if the patient's physician believes that access to the information by the personal representative is reasonably likely to cause harm to the patient or to another person.

## Procedures

- The **Privacy Officer** will review the request to inspect or copy protected health information.
- The **Privacy Officer** will contact the patient's physician to determine if there are any reasons to restrict the patient's or patient representative's access to the information.
- If the request is disapproved, wholly or in part, the patient will be notified using the procedures established by policies [P-5132](#).
- If the request is approved, the patient will be notified and arrangements made for the patient to inspect or copy the requested information using the procedures established by policies [P-5140](#) to [P-5143](#).

### Regulation

#### 45 CFR 164.524(a)(2)

A patient's request to inspect or copy personal health information may always be denied if it involves psychotherapy notes, information used in legal proceedings, or information that cannot be disclosed under the Clinical Laboratory Improvement Amendments (CLIA).

#### 45 CFR 164.524(a)(3)

A patient's request to inspect or copy personal health information maintained by the medical practice may be denied if a licensed health professional has determined that access to the information may result in harm to the patient or to others.

## P-5130 Denial of Requests to Access Protected Health Information

When a patient's request to inspect or copy protected health information is denied, wholly or in part, the patient will be contacted and given an opportunity to request a review of that decision.

Policy [P-5131](#) establishes policies and procedures for communicating the denial to the patient.

Policy [P-5132](#) establishes policies and procedures for reviewing the denial if requested by the patient if requested by patient.

### Regulation

#### 45 CFR 164.524(d)

Establishes procedures for denying requests to inspect or copy protected health information.

## **P-5131 Communication of Denial of Requests for Access to Personal Health Information**

A written explanation of the denial of a patient's request to inspect or copy protected health information will be prepared by completing the appropriate form.

If alternative information can be identified that may partially satisfy the patient's request, including a summary of the requested information, the communication should describe those alternatives.

### **Regulation**

#### **45 CFR 164.524(d)(2)**

Requires written notice and explanation when a request to inspect or copy protected health information is denied.

## **P-5132 Review of Decision to Deny Access**

A patient or patient's representative whose request to inspect or copy protected health information is denied may request a review of that decision by a licensed health professional who was not involved in the decision to deny the request.

### **Procedures**

1. When **Privacy Officer** receives a copy of the denial notice indicating that the patient is requesting a review of the denial, he or she should forward the request to a licensed health professional who was not involved in the original denial and request that physician to review the decision.
2. The review should normally be completed within 30 days. The **Privacy Officer** will follow-up with the reviewing physician if the review is not completed within 30 days of sending him or her the request.
3. The **Privacy Officer** should communicate the result of the review to the patient using the reviewer form.

### **Regulation**

#### **45 CFR 164.524(d)(4)**

When requested by a patient, requires the review of denied requests to inspect or copy protected health information by a person not involved in the original denial.

## **P-5140 Inspection of Records**

If the records must be retrieved from on-site storage, the patient should be notified that the requested information will be made available, generally within 30 days of the date the request was made.

If, however, records must be retrieved from off-site storage, the records should be made available for inspection within 60 days of the submission of the request.

### **Regulation**

#### **45 CFR 164.524(b)(2)**

Establishes timeframes for responding to patient requests for access to protected health information

## **P-5141 Communication of Decision to Permit Inspection or Copying of Protected Health Information**

Approval of a patient's request to inspect or copy protected health information should be communicated to the patient or patient's representative using the request approval form.

The form should specify the earliest date and time that the records will be available for copying.

### **Procedure**

- The **Privacy Officer** will determine the earliest date at which the requested information can be made available.
- The **Privacy Officer** or a designated staff person will prepare the approval form and send it to the patient.

### **Regulation**

#### **45 CFR 164.524(d)**

Establishes requirements for access to protected health information.

### **P-5142 Arrangements for Inspection of Protected Health Information by Patients**

Arrangements should be made to provide access to protected health information at a place and time convenient for the patient.

The patient must inspect the records on the premises of the practice. If this is not satisfactory to the patient, he or she should be given the option of having copies made and sent to an address that he or she specifies. However, the patient must pay for such copies. See policy [P-5143](#).

#### **45 CFR 164.524(c)(3)**

Requires health care providers to provide access in a timely manner at a time and place convenient for the patient.

### **P-5143 Fees for Copying Personal Health Information**

If the patient requests copies of personal health information maintained by the practice, he or she will be charged a flat fee of \$\_ plus \$\_.\_\_ per page.

#### **45 CFR 164.524(c)(4)**

Permits a provider to charge a cost-based fee for copies of protected health information.

### **P-5200 Amendment of Health Information**

A patient may request amendment of the information describing him or her that is maintained by **ProHealth Parters** as part of the designated record sets listed below. The patient must follow the procedures outlined in policy [P-5210](#) when requesting amendment of information maintained by **ProHealth Parters**.

### **Designated Record Sets**

The designated record sets for which a patient may request amendment include:

- The patient's medical records
- The patient's billing records
- Other records that contain protected health information that is used to direct treatment

## Procedures

- The patient must request amendment of protected health information in writing. A form is available for this purpose and should be used. See policy [P-5210](#).
- The request will be reviewed as provided for in policy [P-5220](#).
- If the request is approved, the protected health information will be amended as provided for in policies [P-5230](#) to [P-5232](#).
- If the request is denied, the patient will be notified and offered the opportunity to submit a statement disagreeing with this decision that will be handled using the procedures in policies P-5240 to P-5242.

### Regulation

#### 45 CFR 164.526(a)

Requires providers to allow patients to request amendment of protected health information that they create or maintain.

## P-5210 Procedures for Requesting Amendment of Information

Requests to amend protected health information must be submitted in writing. Patients should use the patient information amendment form.

## Procedures

- Patients who indicate their belief that the information in their records is incorrect should be given a patient information amendment form.
- Patients should be referred to the **Privacy Officer** to resolve questions about the form.

### Regulation

#### 45 CFR 164.526(b)

Permits providers to require written requests for amendment of protected health information.

## P-5220 Action on Requests for Amendment of Information

The **Privacy Officer** may deny a patient's request to amend records if the following criteria are met:

- The information to be amended was not created by **ProHealth Partners**, but was received from another entity
- The information to be amended is accurate and complete
- The information to be amended does not exist in the specified records
- The information to be amended is not available for inspection by the patient or patient's Representative (see policy [P-5100](#)).

Action must be completed on any request for amendment within 60 days of receiving the request. If action cannot be completed within 60 days, the medical practice must notify the patient of the delay, including the reasons for the delay, and complete the review within 90 days of the date the request was originally received.

## Procedures

- Patient information amendment forms should be forwarded to the **Privacy Officer**.
- The **Privacy Officer** should contact the patient's physician or a staff member he or she designates and request a review of the requested amendments.

- The physician or designated staff member should indicate which of the requested amendments should not be made because the information in the patient’s record is accurate and complete or meets the other requirements for denying a request that are listed above.
- The physician or designated staff member should then return the form to the **Privacy Officer** .
- The **Privacy Officer** should review the form after it is returned by the patient’s physician and identify any information that should be amended.
- The **Privacy Officer** should initiate the procedures for amending protected health information specified by [P-5230](#) through [P-5232](#).
- The **Privacy Officer** should prepare a response to the patient as required by policies [P-5240](#) through [P-5242](#).

**Regulation**

**45 CFR 164.526(b)(2)**

Requires providers to take timely action on requests to amend protected health information.

**P-5221 Communication of Decision on Requests for Amendment of Information**

After completing the review of a patient’s request for amendment of protected health information, the **Privacy Officer** will complete the patient information amendment form by indicating the disposition of each requested amendment.

A copy of the completed patient information amendment form will be sent to the patient along with any explanatory comments that the **Privacy Officer** believes to be necessary.

The patient will be asked to submit the names and addresses of any organizations or individuals that he or she has reason to believe have received the uncorrected information for the purpose of notifying them of the amendment.

**45 CFR 164.526(b)(2)**

Requires providers to notify patients of the disposition of requests for amendment of information.

**P-5230 Procedures for Amendment of Records**

When a request for amendment of patient information is approved, the **Privacy Officer** will:

- Initiate the procedures established by policy [P-5231](#) to update the records maintained by the practice.
- Initiate the procedures established by policy [P-5232](#) to explain the amendment to other parties to whom the information had previously been disclosed.

**Regulation**

**45 CFR 164.526(c)**

Requires providers to correct their own records when a request for amendment is approved, to notify the patient of the correction, and to notify others to whom the information affected by the amendment has been disclosed.

**P-5231 Procedures for Amendment of Internal Records**

When a patient’s request for amendment of protected health information is approved, either of the following procedures should be followed:

The records containing the affected information should be updated  
The amended information should be linked to the original information.

## **Procedures**

- The **Privacy Officer** will refer the request for amendment to the medical practice staff member responsible for maintaining the affected records.
- That staff member will identify the records that need to be amended.
- Those records should either be amended or should be linked to the amended information (that is, contained in a new or corrected record where it will be available when the affected information is used or disclosed in the future).

## **Regulation**

### **45 CFR 164.526(c)(1)**

Requires amendment of records maintained by the provider.

## **P-5232 Notification of Recipients of Amended Information**

When a patient's protected health information is amended in response to a request received from the patient, other organizations to which the information being amended has been disclosed will be notified of the amendment.

Organizations to be notified include:

- Business associates, health plans, and other providers that the **Privacy Officer** can identify as having received the information
- Persons and organizations the patient can identify as having received the information that requires amendment, but only to the extent that the **Privacy Officer** can confirm that these persons or organizations received the information
- It is not necessary to confirm that the organizations or other entities notified of the amendment have taken any action to update their own records.

## **Regulation**

### **45 CFR 164.526(c)(3)**

Requires reasonable efforts to notify persons and entities that received the information before it was amended.

## **P-5240 Denial of Request for Amendment**

When a request to amend protected health information is denied, the patient will be informed in writing of the decision. The notice sent to the patient must advise the patient of the following:

- The patient may submit a statement of disagreement that will become part of his or her records and will, in the future, be disclosed to any person or organization that receives the identified information.

- If the patient does not submit a statement of disagreement, he or she may ask the medical practice to include the request for amendment and the denial in any future disclosure of the identified information to any person or organization that receives the identified information.

The patient may file a complaint with the provider concerning the request for amendment (a description of how the patient can file this complaint must be included in the notice).

The letter must identify the name, mailing address, and telephone number of the **Privacy Officer** .

### **Regulation**

#### **45 CFR 164.526(d)(1)**

Specifies the required content of the notice of a denial of the request for amendment that must be sent to a patient.

### **P-5241 Statement of Disagreement**

If the patient disagrees in writing when notified that a request for amendment of protected information has been denied, the **Privacy Officer** will review it and will append it to or otherwise or link it to the patient's record. This will ensure that it will accompany the original information when it is used or disclosed in the future.

The **Privacy Officer** may prepare an accurate summary of the patient's statement of disagreement if he or she believes that a summary will adequately provide a clear understanding of the disputed information.

#### **45 CFR 164.526(5)**

Requires the statement of disagreement or a summary of same to be included with future disclosures of the disputed information.

### **P-5242 Rebuttal of Disagreement**

If a patient disagrees in writing when notified that a request for amendment of protected health information has been denied, the **Privacy Officer** will review the statement and determine whether a formal rebuttal or response, as provided for in federal regulations, is necessary. If it is determined that a rebuttal is necessary, the privacy official will prepare and append it to the patient's records.

### **Procedure**

1. The **Privacy Officer** will consult as necessary with the patient's physician or other medical practice staff members to make this determination.
2. Both the patient's statement of disagreement and the rebuttal statement will be noted in the patient's records.
3. The statement of disagreement and the rebuttal either will be included in the patient's records, or will be linked to those records to permit them to be included with the original information when it is used or disclosed in the future.
4. A copy of the rebuttal statement will be sent to the patient.

### **Regulation**

#### **45 CFR 164.526(d)(4) and (5)**

Requires the patient's statement of disagreement and the rebuttal statement to be attached to the patient's records.

## **P-5250 Receipt of Notification of Amendment**

When a notification of amendment of protected health information is received from another medical practice, health plan, or other covered entity, it will be handled as though it were an amendment approved by the practice.

### **Procedure**

See procedures under policy P-5230.

#### **Regulation**

##### **45 CFR 164.526(e)**

Requires providers to update their records upon receipt of a notification of amendment from another covered entity.

## **P-7000 Accounting for Disclosures**

The policies in this section of the privacy manual establish procedures for developing the Notice of Privacy Practices form and obtaining patient consent to, or authorization of, use and disclosure of protected health information.

#### **Regulation**

##### **45 CFR 164.528**

Requires providers to give patients an accounting of disclosures of protected health information.

## **P-7100 Maintenance of Records of Disclosures**

The **Privacy Officer** will create a system for documenting all disclosures of protected health information for which an individual may request an accounting.

Disclosures of protected health information that a medical practice is not required to report to a patient include:

- Any disclosure for the purpose of treatment, payment, or the day-to-day operation of the practice (i.e., any disclosures of information permitted under the patient's consent to the use and disclosure of protected health information)
- Any disclosure to the patient himself or herself
- Any disclosure for use in a facility directory
- Any disclosure to national security or intelligence agencies that is required by law
- Any disclosure to correctional institutions or law enforcement agencies that is required by law
- Any disclosure that occurred prior to **[April 14, 2003]**, the effective date of the HIPAA privacy rules

#### **Regulation**

##### **45 CFR 164.528(a)(1)**

Requires accounting for disclosures of protected health information with the exception of certain disclosures.

## **P-7210 Procedure to Request an Accounting of Disclosures**

To receive an accounting of disclosures of protected health information, a patient must submit a written request to the **Privacy Officer**.

## **Procedure**

1. A patient who indicates to any medical practice staff member that he or she would like to receive an accounting of disclosures should be told to contact the **Privacy Officer**.
2. The **Privacy Officer** will provide the patient with a disclosure accounting form and review the types of disclosures that will be reported in the accounting.
3. The **Privacy Officer** will determine whether the ability of the patient to obtain an accounting of disclosures has been suspended in response to a request from a law enforcement or health oversight agency.
4. If the patient's right to an accounting has not been suspended, the **Privacy Officer** will initiate the preparation of an accounting as provided for by policy P-7300.

### **Regulation**

#### **45 CFR 164.528(c)**

Requires providers to act on a request for an accounting of disclosures within 60 days.

## **P-7220 Charges for Accountings of Disclosures**

If an individual requests more than one accounting during any 12-month period:

- The individual will not be charged for the first requested accounting in a 12-month period.
- If an individual has received an accounting for which he or she was not charged during the preceding 12 months, he or she will be informed that the practice will charge \$[ \_\_\_\_\_.\_\_ ] for the accounting. If the patient agrees to pay this fee, the accounting will be provided.

### **Regulation**

#### **45 CFR 164.528(c)**

Permits the assessment of fees for certain accountings.

## **P-7230 Suspension of a Patient's Right to Receive an Accounting of Disclosures**

A law enforcement or health oversight agency may request the provider to suspend the right of an individual to request an accounting of disclosures.

Requests from law enforcement agencies should be submitted in writing. The written statement should indicate that providing an accounting is likely to impede the agency's activities and should specify a time period during which the patient's right will be suspended.

A request that is received verbally must be confirmed in writing. If a written request is not submitted, the individual's right to an accounting may be suspended for no more than 30 days.

## **Procedures**

- A communication from a law enforcement or health oversight agency requesting the suspension of a patient's right to an accounting of disclosures should be directed to the **Privacy Officer**.
- The **Privacy Officer** will verify the credentials of the government official that makes a verbal request and document the identity of the official or agency.
- **The Privacy Officer** will place the patient's name on a list of persons whose right to an accounting has been suspended pursuant to an official request.

### **Regulation**

#### **45 CFR 164.528(a)(2)**

Requires a provider to suspend temporarily an individual's right to receive an accounting when requested to do so by a law enforcement or oversight agency.

### **P-7300 Information to Be Provided in an Accounting of Disclosures**

The information that will be provided in an accounting of disclosures includes:

- The date of the disclosure
- The name of the entity or person who received the protected health information
- A brief description of the purpose of the disclosure or a copy of the authorization for the disclosure

**Note:** Disclosures to business associates that are covered under the patient's consent to the use and disclosure for purposes of treatment, payment, and health care operations should not be included in the accounting.

#### **Regulation**

##### **45 CFR 164.528(c)**

Specifies the information that must be included in an accounting of disclosures.

### **P-7400 Documentation of Accountings Provided to Patients**

A copy of any accounting provided to a patient will be retained for a period of six years from the date the accounting is provided.

#### **Regulation**

##### **45 CFR 164.528(d)**

Requires documentation of accountings.

### **P-7500 Documentation of Disclosures Requiring an Accounting**

All disclosures of protected health information that must be included in an accounting of disclosures will be documented by the staff making the disclosure.

#### **Procedure**

- Any disclosure, other than a disclosure covered by the patient's consent to the use and disclosure for purposes of treatment, payment, or health care operations, will be documented by completing a disclosure accounting form.
- The disclosure accounting form will be forwarded to the **Privacy Officer**, who will update the files and databases from which the accounting of disclosures was prepared.

#### **Regulation**

##### **45 CFR 164.528(d)(1)**

Requires documentation of disclosures subject to accounting.

### **P-7575 Destruction/disposal of protected health information**

#### **Policy**

It is the policy of the ProHealth Partners/Argus Medical Management to ensure the privacy and security of protected health information in the maintenance, retention and eventual destruction/disposal of such media.

Destruction/disposal of protected health information will be carried out in accordance with federal and state law, state policy and as defined in our retention policy. The schedule for destruction/disposal shall be suspended for records involved in any open investigation, audit or litigation.

## **Definitions**

### **Protected Health Information/Media:**

- Any record of an individual's health information, regardless of medium or characteristic that can be retrieved at any time.
  - This includes all original consumer records, documents, papers, letters, billing statements, x-rays, films, cards, photographs, sound and video recordings, microfilm, magnetic tape, electronic media and other information recording media, regardless of physical form or characteristic, that are generated and/or received in connection with transacting consumer care or business.

## **Procedures**

- All destruction/disposal of protected health information media will be done in accordance with federal and state law, state policy and following written retention policy/ schedule. Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.
- Records involved in any open investigation, audit or litigation should not be destroyed/disposed of. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for these records until such time as the situation has been resolved. If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order will be obtained to ensure that the records are returned to the organization or properly destroyed/disposed of by the requesting party.
- Records or other documents containing protected health information scheduled for destruction/disposal should be secured against unauthorized or inappropriate access until the destruction/disposal of consumer information is complete. This means that this material should be stored in secure containers (not in wastebaskets, boxes, recycle bins, etc.) until the time of destruction/disposal.
- Contracts between physician(s) and business associates will provide that, upon termination of the contract, the business associate will return or destroy/dispose of all consumer health information. The destruction of protected health information by the Business Associate will be documented in writing and sent to the physician office and are to include:
  - Date of destruction/disposal.
  - Description of the destroyed/disposed record series or medium.
  - Method of destruction/disposal.
  - Inclusive dates covered.
  - A statement that the consumer information records were destroyed/disposed of in the normal course of business.
  - The signatures of the individuals supervising and witnessing the destruction/disposal.
- If such return or destruction/disposal is not feasible, the contract will limit the use and disclosure of the information to the purposes that prevent its return or destruction/ disposal.
- A record of all case files containing protected health information that are destroyed or disposed will be made and retained permanently by physician(s). Permanent retention is required because the records of

destruction/disposal may become necessary to demonstrate that the consumer information records were destroyed/disposed of in the regular course of business. Records of destruction/disposal should include:

- Date of destruction/disposal.
  - Method of destruction/disposal.
  - Description of the destroyed/disposed record series or medium.
  - Inclusive dates covered.
  - A statement that the consumer information records were destroyed/disposed of in the normal course of business.
  - The signatures of the individuals supervising and witnessing the destruction/disposal.
- If destruction/disposal services are contracted or performed by another state agency, the contract or agreement will provide that physician(s) business associate will establish the permitted and required uses and disclosures of information by the business associate as set forth in the federal and state law and include the following elements:
- Specify the method of destruction/disposal.
  - Specify the time that will elapse between acquisition and destruction/disposal.
  - Establish safeguards against breaches in confidentiality.
  - Indemnify physician(s) from loss due to unauthorized disclosure.
  - Require that a non-state government business associate maintain liability insurance in specified amounts at all times the contract is in effect.
  - Provide proof of destruction/disposal.

Consumer information media will be destroyed/disposed of using a method that ensures the consumer information cannot be recovered or reconstructed. Methods of destruction/disposal may be reassessed annually by the security officer, based on current technology, accepted practices, and availability of timely and cost-effective destruction/disposal services.

## **Procedures: Disposal of External Media / Hardware**

### **1. Disposal of External Media**

It must be assumed that any external media in the possession of an employee is likely to contain either protected health information (“PHI”) or other sensitive information. Accordingly, external media (CD-ROMs, DVDs, diskettes, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media which should be shredded and to utilize this policy in its destruction.
- External media should never be thrown in the trash.
- When no longer needed all forms of external media are to be sent to the Privacy Officer or appropriate personnel for proper disposal.
- The media will be secured until appropriate destruction methods are used based on NIST 800-88 guidelines.
- Destruction of External Media shall be logged, and witnessed by Security IT Officer.

## 2. Requirements Regarding Equipment

All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

## 3. Disposition of Excess Equipment

As the older Practice computers and equipment are replaced with new systems, the older machines are held in inventory for a wide assortment of uses:

- Older machines are regularly utilized for spare parts.
- Older machines are used on an emergency replacement basis.
- Older machines are used for testing new software.
- Older machines are used as backups for other production equipment.
- Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.
- Older machines are used to provide a second machine for personnel who often work from home.

### P-8000 Resolution of Complaints and Breaches

The **Privacy Officer** will implement the procedures established in policies P-8100 through [P-8400](#) by which a patient or other individual may file a complaint concerning the privacy policies and procedures that have been adopted by **ProHealth Partners**, or the compliance of staff with those policies.

The **Privacy Officer** also will implement the procedures established in policy [P-8400](#) to mitigate the harmful effect of uses or disclosures of protected health information that violate the privacy policies and procedures established by this manual.

#### Regulation

##### 45 CFR 164.530(d)

Requires covered entities to establish a process to be used by individuals who wish to register complaints about privacy practices or noncompliance with privacy policies and procedures.

### P-8100 Submission of Complaints

A patient or other individual who wants to file a complaint concerning the medical practice's privacy policies and procedures, or a suspected disclosure of protected health information that violates federal or state law should:

- Be directed to the **Office Supervisor** for answers to questions about filing complaints, and
- Receive a copy of the complaint form **PF-9000 – Privacy Complaint Intake Form** from the **Office Supervisor** or **Privacy Officer** to be returned by mail to the address printed on the form, or in person by leaving it with Office Supervisor.

#### Regulation

##### 45 CFR 164.520(b)(1)(vi)

Requires the Notice of Privacy Practices to describe procedures by which an individual may file a complaint.

## **P-8200 Complaint Resolution Procedures**

The **Privacy Officer** will implement the procedures established in policies P-8210, which address resolution of complaints concerning privacy policies and [P-8220](#), which addresses resolution of complaints involving the violation of privacy policies and procedures.

### **Regulation**

#### **45 CFR 164.530(d)(1)**

Requires covered entities to establish a process to be used by individuals who wish to register complaints about privacy practices or noncompliance with privacy policies and procedures.

## **P-8210 Complaints Concerning Privacy Policies and Procedures**

The procedures for resolution of complaints submitted by patients or other individuals concerning the privacy practices of **ProHealth Parters** or the policies and practices established in this manual are outlined below.

### **Procedure**

- Upon receiving a complaint (either a “**HIPAA Incident Report Form**” or a letter outlining a complaint) the **Privacy Officer** or a designated staff member will review the complaint, evaluate the specific details of the complaint, and determine whether the complaint warrants a change in the privacy policies or procedures of the medical practice.
- If a change appears to be warranted, the staff member conducting the evaluation will develop a recommendation and submit it to **Privacy Officer**, who will determine whether an immediate change in policies and procedures is needed to prevent a violation of federal or state privacy standards, laws or regulations.
- If it is determined that a change in policies and procedures is necessary, a revised policy will be prepared following the procedures outlined in policy [P-1520](#). A response should be prepared for signature by **Privacy Officer** and sent to the individual submitting the complaint. The response should thank the individual for his or her interest. It should indicate that the suggestion has been evaluated, and while the practice believes that its current practices comply with federal and state requirements, it is considering changes in privacy practices, policies, and procedures to address the patient’s concerns.
- If a change does not appear to be warranted, a response to the complaint will be prepared for signature by **Privacy Officer**, and sent to the individual submitting the complaint. The response should thank the individual for his or her interest. It should indicate that the suggestion has been evaluated, but that the medical practice believes that its current practices comply with federal and state requirements and are sufficient to protect patient privacy.
- Receipt of the complaint and its final disposition should be documented using the procedures established by policy [P-8300](#).

### **Regulation**

#### **45 CFR 164.530(d)(1)**

Requires covered entities to establish a process to be used by individuals who wish to register complaints about privacy practices and policies and procedures.

## **P-8220 Complaints Arising From Possible Violation of Privacy Policies**

The procedures for resolution of complaints submitted by patients or other individuals concerning the disclosure of protected health information are outlined below.

## Procedure

- A staff member who receives a complaint from a patient or other individual that concerns a possible use or disclosure of protected health information that violates the practice's privacy policies and procedures or that violates federal and state law should *immediately* refer the complaint to **Privacy Officer**.
- The **Privacy Officer** will review the complaint and determine whether a violation occurred, and if so, whether the violation involves only the privacy policies and practices established in this manual, or also involves a violation of federal and state privacy laws and standards.
- If **Privacy Officer** determines the complaint may involve a violation of federal or state standards and legal requirements, he or she will immediately forward the complaint to **ProHealth Partners's** legal counsel for evaluation. The request for evaluation should specify a date by which the evaluation should be completed. The **Privacy Officer** should follow-up and track the status of the referral. If the evaluation indicates that federal or state standards may have been violated, the mitigation procedures established in policy P-8400 should be followed.
- If **Privacy Officer** determines that the complaint does not involve a violation of federal or state standards and legal requirements, he or she will determine whether the medical practice's privacy policies and procedures were violated. If policies and procedures have been violated, the disciplinary procedures established by policy P-1310 should be initiated.
- Upon completion of step 4 **Privacy Officer** should contact the person submitting the complaint and notify him or her of the actions that will be taken to address the complaint.
- Evaluations of complaints should generally be completed within 30 days of receipt.
- The receipt of the complaint and the final disposition should be documented using the procedures established by policy P-8300.

## Regulation

### 45 CFR 164.530(d)(1)

Requires covered entities to establish a process to be used by individuals who wish to register complaints about noncompliance with privacy policies and procedures.

## P-8300 Documentation of Complaints

The **Privacy Officer** will establish and maintain files containing documentation of all complaints received. This documentation will include the actions taken to address or resolve the complaint, including any written correspondence with the person submitting the complaint.

## Procedure

### 45 CFR 164.530(d)(2)

Requires covered entities to document all complaints and their disposition.

## P-8400 Mitigation

When **Privacy Officer** determines that a use or disclosure of protected health information has violated the policies and procedures established by this manual, the case will be referred to **ProHealth Partners** legal counsel to:

- Determine any action needed to mitigate any harm that may result to the patient whose information was used or disclosed
- Evaluate the practice's legal exposure and recommend a course of action
- Follow up with the patient

All communications with the patient concerning use or disclosure of protected health information that legal counsel determines may violate federal or state standards and legal requirements should be handled by the medical practice's legal counsel.

## **Regulation**

### **45 CFR 164.530(f)**

Requires covered entities to mitigate to the extent practicable any harmful effect resulting from the use or disclosure of protected health information that violates the medical practice's policies and procedures, or the requirements of federal law.

### **2009 FTC Red Flag Rule**

Offices will request documents to verify the identity of all patients using Form PF-7000. A valid drivers license can be scanned in color into the CareTracker Dashboard and used each time the patient returns to verify the identity of the patient. If the license is not scanned into CareTracker the actual license or other verification documents must be verified at each visit by the front office staff. Form PF-7000 also requires verification of the identity of a patient representative. This form will remain a permanent part of the patient record. Upon presentation of the documents for validation of the patient's identity, the office staff will look for the following Red Flags which might indicate identity theft:

1. Suspicious documents, such as a forged or altered driver's license or health insurance card.
2. Photographs or a physical description on file not consistent with the appearance of the patient
3. A patient who has an insurance number but never produces a card or other documentation.  
Records showing medical treatment that is inconsistent with a patient's medical history.
4. A notice from a patient or law enforcement entity indicating possible identity theft.
5. A query from a patient regarding a bill or insurance statement for services never received or in another individual's name.
6. Other inconsistent information identifies the patient
7. Inconsistent signatures on file
8. Patient forms or applications appear forged, altered, or destroyed and reassembled
9. Statements sent to the patient or guarantor are returned as un-deliverable despite ongoing transactions on active records.
11. Unusual billing patterns.

A patient whose identity cannot be verified should not be seen until their identity can be verified. A long-time patient who has not exhibited any of the above listed "red flags" while receiving care in your office should not be turned away but any new staff who are not familiar with the patient should still verify the identity of the patient if existing staff who are certain of the patient's identity are not present. A patient who presents verification which meets any of the Red Flag criteria listed above should not be seen by the physician and should be reported to local law enforcement authorities and if the patient's information is already entered into Care Tracker a warning note should be posted for other offices to see.

Office Managers and Supervisors or Regional Managers if there is no Manager or Supervisor, will train all staff on the new policy and procedure for Red Flag Rule compliance.

In the event methods of identity theft change or new risks and trends develop this procedure and policy will be updated.

**END OF HIPAA PRIVACY POLICIES AND PROCEDURES.**

**PRIVACY FORMS AND**

**HIPAA SECURITY POLICIES AND PROCEDURES AND FORMS TO FOLLOW.**

**Form PF-1000**  
**NOTICE OF PRIVACY PRACTICES**

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

**Effective April 14, 2003**

This *Notice of Privacy Practices* is being provided to you as a requirement of the privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This notice describes under what circumstances our medical practice (the Practice") may use and disclose medical information about you to carry out treatment, payment or health care operations and for other purposes that are permitted or required by law. It also describes your rights to access and control medical information about you. Your medical information (i.e., "protected health information" for purposes of HIPAA) is information about you, including demographic information, that may identify you and that relates to your past, present or future physical or mental health or condition. We are required by law to maintain the privacy of your medical information and we must abide by the terms of this notice.

In this notice we provide descriptions of the different ways that we may use and disclose your medical information. In some cases, an example is provided to describe the types of uses and disclosures of your medical information that may be made by us.

In addition to the privacy protections provided under federal law (which are described in more detail below), and except in certain limited circumstances, California law requires us to obtain your written consent (or, under some statutes or rules, written consent from your attorney, guardian, or upon court order) before we can use or disclose your information if you qualify as a patient that:

- Suffers from a sexually transmitted disease;
- Is HIV+ or has Acquired Immune Deficiency Syndrome
- Suffers from a mental disorder;
- Has a problem with substance abuse;
- Is eligible to receive benefits for the State of California for certain developmental disabilities or mental retardation;
- Receives rehabilitative services through the California Medi-Cal program;
- Is eligible to receive certain other benefits through California's Medi-Cal program

**Uses and Disclosures of Protected Health Information**

**For Treatment.** We may use medical information about you to provide you with medical treatment or services. We may disclose medical information about you to doctors, nurses, technicians, residents, or other health care professionals who are involved in taking care of you. For example, we may disclose your medical information to another doctor or healthcare provider (such as a specialist, your primary care doctor, a pharmacist or clinical laboratory) who, at the direction of your doctor, is involved in your treatment or care. California Law may also limit these uses or disclosures of your medical information.

**For Payment.** We may use and disclose medical information about you so that the treatment and services you receive may be billed to and payment may be collected from you, an insurance company or others. For example, your insurance company may need to know certain information about the diagnostic test (such as a stress test or electrocardiogram) or procedure (such as a sigmoidoscopy or conization) you received so they will pay us or reimburse you for the test or procedure. We may also use and disclose medical information about you to obtain prior approval or to determine whether your insurance company will cover a proposed treatment. California Law may also limit these uses or disclosures of your medical information.

**For Health Care Operations.** We may use and disclose medical information about you, for health care operations. This is necessary to make sure that all of our patients receive quality care and to support the business operations of our Practices. These uses or disclosures of your medical information may also be limited by California Law.

A few examples of our health care operations are quality improvement, doctor/employee review activities, compliance, and the training of health care professionals. Also included in healthcare operations are the day-to-day tasks that are required to keep our Practice locations functioning and to provide you with quality care.

For example, in the waiting room when your doctor is ready to see you. In addition, we may contact you (e.g., by telephone or mail) to remind you about an appointment, to provide instructions prior to a diagnostic test or procedure, to provide information about treatment alternatives, or other health-related benefits that may be of interest to you, or to discuss your account.

In such cases, we may leave a message on your answering machine, if available. The departments that may have reason to communicate with you regarding your care include the following:

- Reception/Communications (i.e., appointment reminders)
- Diagnostic Testing
- Authorizations
- Research
- Clinical Services
- Business Office
- Quality Improvement (i.e., patient satisfaction)

As another part of health care operations, we may use and disclose medical information about you to our "business associates". Our business associates, such as transcription services, collection agency, and call answering service, just to name a few, perform services on behalf of the Practice. Whenever an arrangement between our Practices and a business associate involves the use or disclosure of medical information about you, we will have a written contract with that business associate that will require such business associate to agree to protect the privacy of your medical information.

### **Uses and Disclosures of Protected Health Information Not Discussed in This Notice**

Uses and disclosures of your medical information that have not been described in this notice will not be made without your written permission. If you provide us permission to use or disclose medical information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose medical information about you for the reasons covered by such permission. However, you should understand that we are unable to take back any actions we have already taken with your permission, and that we are required to retain our records of the care we provided to you.

### **Other Permitted and Required Uses and Disclosures That May Be Made With Your Agreement or Opportunity to Object**

You have the opportunity to agree or object to the use or disclosure of all or parts of medical information about you in the situations discussed in the following paragraphs. If you are not present or able to agree or object to the use or disclosure of your medical information in such instances, then your doctor may, using his or her professional judgment, use or disclose your medical information if believed to be in your best interest. California Law may also limit these uses or disclosures of your medical information.

**Individuals Involved in Your Care or Payment for Your Care.** Unless you object, in an urgent situation we may release medical information about you to a friend, family member, or any other person you identify who is involved in your medical care. We may also give information to someone who helps pay for your care. We may use or disclose medical information about you to notify or assist in notifying a family member, personal representative or any other person that is responsible for your care of your location, general condition or death. In addition, we may disclose medical information about you to an entity assisting in a disaster relief effort so that your family can be notified about your location, general condition or death.

### **Research**

We may use and disclose medical information about you for research purposes under certain circumstances. However, other than obtaining medical information in preparation for a research program or protocol, your specific permission is generally required if such research will involve the use or disclosure of your medical information.

### **Other Permitted and Required Uses and Disclosures That May Be Made Without Your Authorization or Opportunity to Agree or Object**

Unless California Law requires otherwise, we may use or disclose your protected health information in certain situations without your specific permission or without giving you an opportunity to agree or object. Among these situations are the following:

**Required By Law.** We are permitted to disclose medical information about you when required to do so by federal, state or local law.

**To Avert a Serious Threat to Health or Safety.** In certain circumstances, we may use and disclose medical information about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person.

**To Notify an Employer of Medical Information Related to an Employee:**

- or to evaluate whether an employee has a work-related injury or illness,
- the use or disclosure of information is related to these purposes,
- the use and disclosure is required for the employer to comply with its legal obligations,
- and the covered entity was providing services at the request of an employer for medical surveillance the
- employee is given notice that the information will be disclosed (notice can be handed to patient)

**Military and Veterans.** If you are a member of the armed forces, in certain circumstances we may release information about you to an appropriate government body.

**Workers' Compensation.** We may release medical information about you to comply with workers' compensation (or similar) laws.

**Inmates.** If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may in certain circumstances release medical information about you to the correctional institution or law enforcement official. .

**Public Health Activities.** We may disclose medical information about you for public health activities. These activities generally include, without limitation, the following:

- to prevent or control disease, injury or disability;
- to report births and deaths;
- to report child abuse and neglect;
- to report animal bites;
- to report reactions to medications or problems with products;
- to notify people of recalls or products they may be using;
- to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading disease or condition, or
- to notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence

**Health Oversight Activities.** We may disclose medical information to a health oversight agency for activities related to the monitoring of the health care system, government programs or compliance with civil rights laws. These oversight activities include; for example, audits, investigations, inspections, and licensure.

**Lawsuits and Disputes.** In certain circumstances, we may disclose medical information about you in response to a subpoena, discovery request, or other lawful order from a court.

**Law Enforcement.** We may release medical information if asked to do so by a law enforcement official as part of law enforcement activities in certain circumstances.

**Coroners, Medical Examiners and Funeral Directors.** If authorized by law, we may release medical information to a coroner or medical examiner. We may also release medical information to a funeral director, as consistent with applicable law, in order to permit the funeral director to carry out his or her duties. Also, medical information may be used and disclosed for organ, or tissue donation purposes.

**Protective Services for the President, National Security and Intelligence Activities.** We may disclose medical information about you to authorized federal officials so they may, without limitation, (i) provide protection to the President; other authorized persons or foreign heads of state or conduct special investigations, or (ii) conduct lawful intelligence, counter-intelligence, or other national security activities authorized by law.

**Your Rights Regarding: Medical Information We Maintain About You**

**Right to Inspect and Copy.** You have the right to inspect and copy medical information that relates to you. To do so, you must submit your request in writing to our Privacy Officer at the address below. If you request a copy of the information, we may charge you a reasonable fee for the costs of copying, mailing or other supplies associated with your request.

We may deny your request to inspect and copy in certain circumstances. If you are denied access to medical information, you may in certain circumstances request that the denial be reviewed. In such cases, another licensed health care professional chosen by ProHealth/Argus will review *your* request and the denial. The person conducting the review will not be the person who denied your request. We will comply with the outcome of the review.

**Right to Amend.** If you feel that medical information we have about you is incorrect or incomplete, you may ask us to amend the

information. In certain circumstances, you have the right to amend your medical information.. Your request for an amendment must be made in writing and submitted to our Privacy Officer at the address below. In addition, you must provide a reason that supports your request. We may deny your request for an amendment in certain circumstances.

**Right to an Accounting of Disclosures.** You have the right to receive an accounting of certain disclosures that we have made. To request an accounting of disclosures, you must submit your request in writing to our Privacy Officer at the address below. Your request must state a time period that may not be longer than six (6) years and may not include dates before April 14, 2003. Your request should indicate in what form you want the list (for example, on paper or electronically). The first list you request within a 12-month period will be free. For additional lists within a single 12-month period, we may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

**Right to Request Restrictions.** You have the right to request a restriction or limitation on how we use or disclose certain medical information about you, including how we use or disclose your medical information *for* treatment, payment or health care operations. To request restrictions, you must make your request in writing to our Privacy Officer at the address below. In your request, you must tell us: 1) what information you want to limit; 2) whether you want to limit our use, disclosure or both; and 3) to whom you want the limits to apply. We are not required to agree to your request. If we do agree, we will comply with your request unless the information is needed to provide you emergency treatment.

**Right to Request Confidential Communications.** You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail. To request confidential communications, you must make your request in writing to our Privacy Officer at the address below. We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

**Right to a Paper Copy of This Notice.** You have the right to a paper copy of this notice at any time. Even if you have agreed to receive this notice electronically, you are still entitled to a paper copy of this notice. To obtain a paper copy of this notice, you can request one in writing from our Privacy Officer at the address below or simply ask for a copy at the reception/check-in desk at your doctor's office.

**Right to receive notification of any breach of your unsecured PHI.**

**Right to request restrictions on PHI disclosures to your health plan for health services or items paid out-of-pocket in full**

**Right to opt out of fundraising communications**

**Right to authorize disclosures for marketing purposes, including subsidized treatment communications**

**Right to authorize other uses and disclosures not described in the NPP including disclosures of PHI that constitute the sale of PHI.**

**Right to authorize disclosures of psychotherapy notes**

### Changes to his Notice

We reserve the right to change this notice at any time. We reserve the right to make the revised or changed notice effective for medical information we already have about you as well as any information we receive in the future. We will post a copy of the current notice. The notice will contain on the first page, in the bottom right-hand corner, the effective date.

### Complaints

If you believe your privacy rights have been violated, you may file a complaint with us or with the Secretary of the Department of Health and Human Services. To file a complaint, contact our Privacy Officer at the address below. All complaints must be submitted in writing. You will not be penalized for filing a complaint, and we will seek to deal with all complaints in a reasonable and efficient manner.

**Privacy Officer:** Linda Grow, HIPAA Compliance Officer

ProHealth Partners/Argus Medical Management  
5150 E. Pacific Coast Highway #500, Long Beach CA 90804  
(562) 299-5203 Phone Fax No. (562) 299-5204 Email [lgrow@argusmso.com](mailto:lgrow@argusmso.com)

**Form PF-2000**  
**Acknowledgement of Receipt of Notice of Privacy Practices**

*The Practice reserves the right to modify the privacy practices outlined in this notice.*

I have received a copy of the Notice of Privacy Practices which is also posted in the reception area of this office. I may receive a copy of an amended notice upon request at subsequent visits. This notice can also be found and downloaded from [www.prohealthpartners.com](http://www.prohealthpartners.com)

\_\_\_\_\_  
Name of patient (Print or Type)

\_\_\_\_\_  
Signature of Patient

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature of Patient Representative  
(Required if patient is a minor or an adult who is unable to sign this form)

\_\_\_\_\_  
Relationship of Representative

---

---

**Documentation of Attempt to Obtain Acknowledgement of Receipt of  
Privacy Practices**

An attempt was made to obtain an acknowledgement of the Notice of Privacy Practices on

\_\_\_\_\_. The acknowledgement was not obtained because:

Date

- The patient was undergoing emergency treatment
- The patient declined to sign the acknowledgement
- Other \_\_\_\_\_

Signature: \_\_\_\_\_

Name of the patient: \_\_\_\_\_

Name of Staff Member: \_\_\_\_\_

Date: \_\_\_\_\_



PF 3000

\_\_\_\_\_  
\_\_\_\_\_  
Doctor Name  
Office Address



**AUTHORIZATION FOR USE AND/OR DISCLOSURE OF PROTECTED HEALTH INFORMATION**

**(Do Not Use This Form If Records To Be Released Relate to HIV Test Results, Mental Health or Alcohol/Drug abuse)**

EXPLANATION: This Authorization is necessary for us to comply with state and federal laws pertaining to the use or disclosure of protected health information ("PHI") about the patient identified below. Please provide all requested information. Failure to provide all requested information may prevent us from acting on this Authorization.

Name of Patient: \_\_\_\_\_ Date of Birth: \_\_\_\_\_

Other Names: \_\_\_\_\_ Account #: \_\_\_\_\_

1. PERSONS AUTHORIZED TO DISCLOSE PHI. I authorize the following person(s) or class of persons to disclose the health information about patient as described in Section 2 below: *(State name of physician or specific identification of person or class of persons)* \_\_\_\_\_

2. DESCRIPTION OF INFORMATION. This Authorization permits the use and/or disclosure of the following information about patient: *(Check all applicable boxes and initial selection as required)*.

\_\_\_\_\_ (Initial) All my health information marked below pertaining to any medical history, physical condition and treatment received. Except *(optional)*: \_\_\_\_\_

Medical Office Records  Hospital Records  X-ray films & images  Laboratory Results

Or, only the following records or types of health information and/or only on the specified date(s):

Date(s) of Treatment: \_\_\_\_\_ Type of Treatment: \_\_\_\_\_

\_\_\_\_\_ (Initial) Other \_\_\_\_\_

3. AUTHORIZED USERS AND RECIPIENTS. I hereby authorize the following person or class of persons to receive and/or use the health information described in Section 2 above: *(State name and title if applicable.)* **Name:** \_\_\_\_\_ **Title** (if applicable) \_\_\_\_\_

Address: \_\_\_\_\_ City, State, Zip \_\_\_\_\_

4. PURPOSE. I hereby authorize the information checked in Section 2 above to be used and/or disclosed for the following purposes: *(Check all applicable boxes)(Researchers should note that this must be research study specific, not for future unspecified research release)*

Requested by patient or personal representative.  Other: \_\_\_\_\_

Physician or practice will be remunerated for this information. Yes  No

5. RIGHT OF REVOCATION. I understand that I have the right to revoke this authorization at any time, providing that my revocation is in writing and conforms to requirements described in the ProHealth Partners/Argus Notice of Privacy Practices.
6. LIMITS TO REVOCATION. I understand that my revocation will be effective upon its receipt by the person(s) I authorized in Section 1 but would not be effective to the extent that such persons have acted in accordance with this Authorization and in reliance thereon. With respect to the person(s) I authorized to receive and use health information described in Section 3, if patient (or personal representative) requested the Authorization, any revocation will be effective only when I communicate my revocation directly to them.
7. REDISCLOSURE. I understand that if the recipient of my information in Section 3 above is not a healthcare provider, a health plan or a health care clearing house or not an entity required to comply with federal or state health privacy regulations, my health information may be further disclosed by such recipient and my information may no longer be protected by state and federal laws. If this Authorization is for the disclosure of substance abuse information, the recipient may be prohibited from disclosing the substance abuse information under federal substance abuse confidentiality requirements.
8. CALIFORNIA RESTRICTIONS. I understand that a recipient of medical information in California may not further disclose medical information about me (patient) unless a new Authorization form is signed by me or my personal representative or unless the disclosure is specifically required or permitted by law.
9. RIGHT TO REFUSE TO SIGN. I understand that I do not have to sign this authorization and that my failure to sign this authorization will not affect my ability to obtain treatment, payment or benefits.
10. AUTOMATIC ONE-YEAR DURATION. This authorization will automatically expire after one (1) year from date of execution unless a different end date or event is specified.  
End date \_\_\_\_\_ Or Event \_\_\_\_\_
11. COPY RECEIVED. I acknowledge receipt of a signed copy of this authorization \_\_\_\_\_ (Initials)

\_\_\_\_\_  
Signature of Patient or Personal Representative

\_\_\_\_\_  
Date

\_\_\_\_\_  
Print name of Personal Representative (if applicable)

\_\_\_\_\_  
Relationship of Personal Rep. to Patient

\_\_\_\_\_  
Address

\_\_\_\_\_  
Phone number

\_\_\_\_\_  
Type of pt./rep. ID presented. Attach copy (optional)

\_\_\_\_\_  
Verified Yes No Initials who verified

ATTENTION RECIPIENT: ANY DISCLOSURE OF MEDICAL RECORD INFORMATION BY THE RECIPIENT IS PROHIBITED EXCEPT WHEN IMPLICIT IN THE PURPOSE OF THIS DISCLOSURE



\_\_\_\_\_ Doctor Name  
\_\_\_\_\_ Office Address



**Form PF-4000 Tracking of Request for Access or Disclosure of PHI**

**ACCOUNTING OF DISCLOSURES TRACKING SHEET**

Use this form to track all disclosures outside of Treatment, Payment and Health Care Operations (TPO) for the Patient Listed Below. Our practice must keep and be prepared to make this information available to the patient, upon their request, for a period of six (6) years.

**NAME OF PATIENT** \_\_\_\_\_ **DATE OF BIRTH** \_\_\_\_\_

Date Information Was Released:
To whom was the information (PHI) released/disclosed:
Description of the information released/disclosed:
Additional Information/Notes:
Reported By: _____ Signature: _____

Date Information Was Released:
To whom was the information (PHI) released/disclosed:
Description of the information released/disclosed:
Additional Information/Notes:
Reported By: _____ Signature: _____

Date Information Was Released:
To whom was the information (PHI) released/disclosed:
Description of the information released/disclosed:
Additional Information/Notes:
Reported By: _____ Signature: _____

**AUTHORIZATION TO COMMUNICATE PATIENT'S MEDICAL INFORMATION**

COMMUNICATION WITH FAMILY & OTHERS INVOLVED IN YOUR CARE

(Signed original to be placed in the central medical record and copy to patient)

<b><u>PATIENT IDENTIFICATION</u></b>
Name: _____
Date of birth: _____
S.S. #: _____
Medical Record/Account#: _____

Office Name: _____
Address: _____
City/State/Zip: _____
Phone number: _____
Fax number: _____
Physician name: _____

Please list any family members or others who may be involved in coordinating your care or payment for care. Also, indicate what kinds of information may be shared with each individual.

NAME:	RELATIONSHIP TO PATIENT	TYPE OF INFORMATION			
		ALL	Scheduling/ Appointment	Medical	Billing/ Insurance

Specific instructions or limitations: \_\_\_\_\_

\_\_\_\_\_

Validation code: \_\_\_\_\_ (Please give this to any individual who may be involved in coordinating your care or payment for care. They will be asked to give this code to our staff before we release information over the phone.)

We will continue to rely on the information on this form when communicating with family members or others involved in your care unless you request changes. **You are authorizing those listed to receive your protected health information.** Please promptly notify your physician's office if you wish to alter the designations above.

Signature of Patient/Legal Representative: \_\_\_\_\_ Date: \_\_\_\_\_

Relationship to patient: \_\_\_\_\_



Form PF-6000  
HIPAA FORM FOR  
RECORDS DESTRUCTION



OFFICE NAME: \_\_\_\_\_

OFFICE ADDRESS: \_\_\_\_\_

PHYSICIAN NAME(S): \_\_\_\_\_

**CERTIFICATE OF DESTRUCTION**

**The information described below was destroyed in the normal course of business pursuant to the organizational retention schedule and destruction policies and procedures.**

Date of Destruction:	Authorized By:
Description of Information Disposed Of/Destroyed:	
Inclusive Dates Covered:	
<b>METHOD OF DESTRUCTION:</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Burning</li> <li><input type="checkbox"/> Overwriting</li> <li><input type="checkbox"/> Pulping</li> <li><input type="checkbox"/> Pulverizing</li> <li><input type="checkbox"/> Reformatting</li> <li><input type="checkbox"/> Shredding</li> <li><input type="checkbox"/> Other: _____</li> </ul>	
Records Destroyed By*:	
If On Site, Witnessed By:	
Department Manager:	

*\*If records destroyed by outside firm, you must confirm a Business Associate Agreement exists*



Form PF-7000  
HIPAA FORM FOR  
VERIFICATION OF IDENTITY



OFFICE  
NAME: \_\_\_\_\_

OFFICE  
ADDRESS: \_\_\_\_\_

PHYSICIAN  
NAME(S): \_\_\_\_\_

**VERIFICATION OF PATIENT IDENTIFICATION**

Name: \_\_\_\_\_ Document verifying name: \_\_\_\_\_  
*Document verifying name must not appear altered or forged*

Date of birth: \_\_\_\_\_ Document verifying DOB: \_\_\_\_\_  
*Document verifying DOB must not appear altered or forged*

S.S. #: \_\_\_\_\_ Document verifying SS#: \_\_\_\_\_  
*Document verifying SS# must not appear altered or forged*

California Drivers license # \_\_\_\_\_ Other State and # \_\_\_\_\_

Photograph copied to chart  Yes  No (if no, see below)  
*Patient must have photo identification or see below*

Physical Description entered in chart  Yes  No

**VERIFICATION OF PATIENT'S AUTHORIZED REPRESENTATIVE**

**1. Must have proof of authorization to receive information. Document should not appear forged, altered or destroyed and re-assembled. Verify patient signature.**

**2. Must have photo identification to verify their identity prior to release of information.**

## **RED FLAGS THAT MIGHT INDICATE IDENTITY THEFT**

*The FTC and other experts have identified examples of these warning signs, including:*

- 1. Suspicious documents, such as a forged or altered driver's license or health insurance card.**
- 2. Photographs or a physical description on file are not consistent with the appearance of the patient**
- 3. A patient who has an insurance number but never produces a card or other documentation.**
- 4. A query from a patient regarding a bill or insurance statement for services never received or in another individual's name.**
- 5. Records showing medical treatment that is inconsistent with a patient's medical history.**
- 6. A notice from a patient or law enforcement entity indicating possible identity theft.**
- 7. Unusual billing patterns.**
- 8. Other inconsistent information identifies the patient**
- 9. Inconsistent signatures on file**
- 10. Patient forms or applications appear forged, altered, or destroyed and reassembled**
- 11. Statements sent to the patient or guarantor are returned as un-deliverable despite ongoing transactions on active records**

**A patient whose identity cannot be verified should not be seen until their identity can be verified. A long-time patient who has not exhibited any of the above listed "red flags" while receiving care in your office should not be turned away but any new staff who are not familiar with the patient should still verify the identity of the patient if existing staff who are certain of the patient's identity are not present. A patient who presents verification which meets any of the Red Flag criteria listed above should not be seen by the physician and should be reported to local law enforcement authorities and if the patient's information is already entered into Care Tracker a warning note should be posted for other offices to see.**



Form PF-8000  
HIPAA INCIDENT REPORT FORM



**INCIDENT DATE:** \_\_\_\_\_ **REPORT DATE:** \_\_\_\_\_

**PATIENT NAME:** \_\_\_\_\_ **PHYSICIAN NAME:** \_\_\_\_\_

***IF MULTIPLE PATIENTS, LIST ON SEPARATE PAPER AND ATTACH***

**STAFF NAME COMPLETING REPORT:** \_\_\_\_\_

**STAFF NAME(S) INVOLVED IN ERROR:** \_\_\_\_\_

**NATURE OF INCIDENT:**  Rx/SureScripts Error  Lab/Diagnostic Report  Medical Record

Correspondence  Other, please explain any of these incidents in detail below.

---

---

---

---

---

---

---

---

**CONSEQUENCE OF THE ERROR:** (i.e. patient received wrong Rx, wrong Lab Report, etc.)

---

---

---

**CORRECTIVE ACTION PLAN:** *(Work with HIPAA Privacy Officer to develop plan to prevent recurrence)*

---

---

---

---

---

**CORRECTIVE ACTION TIMEFRAME:**  Immediately  One Week  Two Weeks  One Month

**DATE FOR COMPLETION:** \_\_\_\_\_ **DATE COMPLETED:** \_\_\_\_\_

**COPY THIS REPORT TO:** PHYSICIAN, REGIONAL MANAGER, PRIVACY OFFICER/RISK MANAGER

## Requirements for breach notification and sample letter to patient.

HIPAA guidelines: These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

On physician letterhead:

Date of the letter: \_\_\_\_\_

Re: Breach of protected health information

Dear Patient,

Description of the breach including date: \_\_\_\_\_

Information involved in the breach: \_\_\_\_\_

You should take steps to protect your identity from potential harm, such as notifying your health plan of the theft to prevent fraudulent use of your health benefits and for the personal identity information, enlisting the services of an identity protection service, like LifeLock or [IDENTITY GUARD](#).

You may contact the Privacy Officer for additional information or for answers to your questions about this event.

Linda Grow  
Privacy Officer  
562-299-5203 telephone  
[lgrow@argusmso.com](mailto:lgrow@argusmso.com)  
5150 E. Pacific Coast Highway, Suite 500  
Long Beach, CA 90804

We sincerely apologize for any inconvenience.

Sincerely,  
Physician name here

**HIPAA FORM PF-9000**

**PRIVACY COMPLAINT INTAKE FORM**

Date of the Complaint:

**Information on the person filing the complaint:**

Name

Address

City, State, Zip Code

Date of the Incident  Time of the incident

Location of the Incident

Persons Involved

Nature of the Breach

Harm to the patient

Statement by  
Person Making  
the Complaint

Statement by  
Any Witnesses

Person(s) Notified

**LEVEL OF OFFENCE:**

- \_\_\_\_\_ Level 1 – A single designated person can resolve the issue in a short amount of time.
- \_\_\_\_\_ Level 2 – The incident requires the attention of other staff.
- \_\_\_\_\_ Level 3 – This is a serious security incident requiring an organized response team.

Identified  
Privacy/Security  
Deficiency

Determination  
as to how the  
incident could  
have been  
prevented

Determination  
as to the  
appropriate  
corrective  
action

Reviewed by

Date

Signature Field

This incident has been resolved according to practice policies and procedures.



PF-9500



## REQUEST FOR RESTRICTION ON USE/DISCLOSURE OF PHI

**TO OUR PATIENTS:** You have the right to request that we restrict our use and disclosure of your protected health information. This means you may ask us not to use or disclose any part of your PHI for purposes of treatment, payment or health care operations. You may also request that any part of your PHI not be disclosed to family members or friends who may be involved in your care or for notification purposes as described in the Notice of Privacy Practices.

Your request must state the specific restriction requested and to whom you want the restriction to apply. We are not required to agree to a restriction that you may request.

We must agree not to disclose your PHI to your health plan if the disclosure is for payment or health care operations and relates to a health care item or service which you paid for in full out of pocket. If we agree to the requested restriction, we may not use or disclose your PHI in violation of that restriction unless it is needed to provide emergency treatment.

We reserve the right to terminate your requested restriction if:

- You agree to termination of the restriction, either in writing or verbally; or
- You requested the termination yourself.

**Patient Name:** \_\_\_\_\_

**Street or PO Box:** \_\_\_\_\_

**City:** \_\_\_\_\_ **State:** \_\_\_\_\_ **Zip:** \_\_\_\_\_

**Phone Number (day):** \_\_\_\_\_

**1) Protected Health Information to be restricted:** \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**2) Nature of Restriction:** \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Patient Name** \_\_\_\_\_

(PLEASE PRINT)

**Signature of Patient** \_\_\_\_\_ **Date** \_\_\_\_\_

(REQUIRED)

THIS SECTION FOR INTERNAL USE ONLY

Request to restrict PHI has been: \_\_\_\_\_ Accepted \_\_\_\_\_ Denied

## INDEX OF TOPICS

### PAGE

<u>1</u>	<b>Cover page</b>
<u>2</u>	<b>P-1000 General Administrative Policies and Procedures</b> <b>P-1100 Staff Responsibilities to safeguard privacy of patient information</b> <b>P-1110 Designation of Privacy Official</b>
<u>3</u>	<b>P-1120 General Staff Responsibilities</b> <b>P-1130 Authority and Responsibility of Individual Staff Members</b> <b>P-1200 Staff Training</b>
<u>4</u>	<b>P-1210 Content of Privacy Training Program for Staff</b> <b>P-1220 Initial Privacy Orientation and Training</b>
<u>5</u>	<b>P-1230 Revised Policy and Procedure Training</b> <b>P-1300 Staff Compliance and Sanctions</b> <b>P-1310 Reporting of Suspected Violations of Privacy Policies and Procedures</b>
<u>6</u>	<b>P-1311 Sanctions and Penalties against staff members who violate privacy policies &amp; procedures</b> <b>P-1312 Investigation of Potential Privacy Violations by Staff Members</b>
<u>7</u>	<b>P-1313 Sanctions and Penalties for Technical Violations Not Involving Use and Disclosure</b> <b>P-1314 Sanctions and Penalties for Unintentional Violations Involving Use and Disclosures</b>
<u>8</u>	<b>P-1315 Sanctions and Penalties for Intentional Violations Involving Use and Disclosures</b> <b>P-1316 Protection of Whistleblowers</b> <b>P-1320 Documentation of Sanctions Brought Against Employees</b>
<u>9</u>	<b>P-1400 Business Associates and Protected Information</b>
<u>10</u>	<b>P-1410 Duty of Staff to Report Contractual Breaches by Business Associates</b> <b>P-1420 Investigation and Correction of Contractual Breaches</b>
<u>11</u>	<b>P-1430 Reporting of Contractual Breaches by Business Associates</b> <b>P-1500 Development and Maintenance of Privacy Policies and Procedures</b>
<u>12</u>	<b>P-1510 Responsibility for Developing and Updating the Privacy Manual</b> <b>P-1520 Procedures for Updating Privacy Policies and Procedures</b>
<u>13</u>	<b>P-1530 Approval of Policies and Procedures</b> <b>P-1540 Communication and Implementation of Revised Policies and Procedures</b> <b>P-1600 Documentation and Record-Keeping</b>
<u>14</u>	<b>P-1610 Establishment of Record-Keeping Systems</b> <b>P-1620 Maintenance of Written Records</b> <b>P-1630 Retention of Records and Documentation</b>

- 15** P-2000 Use and Disclosure of Protected Health Information
  - P-2100 Use and Disclosure of Information for Treatment Purposes
  - P-2110 Provision of Notice Prior to Non-emergency Treatment
  - P-2120 Sharing Information Outside the Practice
- 16** P-2130 Requesting Information From Outside the Practice
  - P-2200 The Use of Patient Information for Payment Purposes
- 17** P-2210 Definition of Payment Activities
  - P-2212 Application of Minimum Necessary Standard to Payment
  - P-2300 The Use and Disclosure of Information for Health Care Operations
- 18** P-2310 Definition of Health Care Operations
  - P-2400 Law Enforcement and Public Health
    - P-2410 Disclosure of Patient Information to Public Health Agencies
- 19** P-2420 Reporting of Abuse, Neglect, and Domestic Violence
- 20** P-2421 Mandatory Reporting of Child Abuse and Neglect
- 21** P-2422 Mandatory Reporting of Abuse, Neglect, and Domestic Violence
  - P-2423 Non-mandatory Reporting of Abuse, Neglect, and Domestic Violence
- 22** P-2424 Voluntary Reporting of Abuse, Neglect, and Domestic Violence with the Patient's Agreement
  - P-2425 Informing Patients of Disclosures
  - P-2430 Disclosure of Patient Information to Law Enforcement Agencies
- 23** P-2440 Disclosure of Patient Information to Oversight Agencies
  - P-2450 Disclosures Related to Judicial and Legal Actions
    - P-2451 Procedure for subpoena requesting billing information
- 24** P-2500 Marketing and Fundraising
  - P-2510 Marketing Communications That Require Authorization
- 25** P-2520 Marketing Activities That Require Authorization
  - P-2530 Fundraising Activities
- 26** P-2600 Other Disclosure Situations
  - P-2610 Disclosure of Information for the Purpose of Cadaveric Organ Donation
  - P-2620 Disclosure of Information to Coroners and Medical Examiners
- 27** P-2630 Disclosure of Information to Funeral Directors
  - P-2640 Disclosure to Avert a Threat to Health or Safety
- 28** P-2650 Disclosure to Disaster Relief Agencies
  - P-2700 Disclosure of Protected Health Information After Death
  - P-3000 Notice and Authorization

	P-3100 Notice of Privacy Practices
<b>29</b>	P-3100 Notice of Privacy Practices continued
<b>30</b>	P-3120 Providing the Notice of Privacy Practices to Patients
	P-3190 Acknowledgment of the Notice
<b>31</b>	P-3300 Authorization of Use or Disclosure
<b>31 - 33</b>	P-3310 Elements of a Valid Authorization
<b><u>33</u></b>	P-3320 Obtaining Authorization for Use or Disclosure
<b><u>34</u></b>	<u>P-3330 Patients' Refusal to Sign an Authorization Form</u>
<b>34 - 35</b>	P-3340 Revoking Authorization for Use or Disclosure
<b><u>35</u></b>	P-3400 Patient Requests for Restrictions on Uses and Disclosures and Confidential Communications
<b>35 - 36</b>	P-3410 Patient Requests for Restrictions on Use and Disclosure
<b><u>36 - 37</u></b>	P-3411 Termination of Restrictions On Use and Disclosure
<b><u>37 - 38</u></b>	P-3420 Patient Requests for Confidential Communication
<b><u>38</u></b>	P-4000 Personal Representatives, Parents, Spouses and Others
	P-4100 Personal Representatives
<b>39</b>	P-4110 Designation of a Personal Representative
	P-4120 Authority of Personal Representative
<b>39 - 40</b>	P-4130 Refusal to Recognize Personal Representative
<b><u>40</u></b>	P-4200 Parental Access to Protected Health Information Concerning Children
<b>40 - 41</b>	P-4300 Disclosure of Information to Family Members and Relatives
<b><u>41</u></b>	P-4400 Disclosure of Information to Close Personal Friends
<b>42</b>	P-5000 Patient Access to Health Information
<b><u>42</u></b>	P-5100 Patient Requests for Access to Protected Health Information
<b>42</b>	P-5110 Request for Access to Protected Health Information
<b><u>43</u></b>	P-5120 Review of Patient Requests for Access to Protected Health Information
<b><u>44</u></b>	P-5130 Denial of Requests to Access Protected Health Information
<b>44</b>	P-5131 Communication of Denial of Requests for Access to Personal Health Information
<b>45</b>	P-5132 Review of Decision to Deny Access
<b><u>45</u></b>	P-5140 Inspection of Records
<b>45</b>	P-5141 Communication of Decision to Permit Inspection or Copying of Protected Health Information
<b>46</b>	P-5142 Arrangements for Inspection of Protected Health Information by Patients
<b><u>46</u></b>	P-5143 Fees for Copying Personal Health Information

<b>46</b>	<b>P-5200 Amendment of Health Information</b>
<b>47</b>	<b>P-5210 Procedures for Requesting Amendment of Information</b>
<b><u>47</u></b>	<b>P-5220 Action on Requests for Amendment of Information</b>
<b>48</b>	<b>P-5221 Communication of Decision on Requests for Amendment of Information</b>
<b><u>48</u></b>	<b>P-5230 Procedures for Amendment of Records</b>
<b>48</b>	<b>P-5231 Procedures for Amendment of Internal Records</b>
<b><u>49</u></b>	<b>P-5232 Notification of Recipient's of Amended Information</b>
<b>49</b>	<b>P-5240 Denial of Request for Amendment</b>
<b><u>50</u></b>	<b>P-5241 Statement of Disagreement</b>
<b>50</b>	<b>P-5242 Rebuttal of Disagreement</b>
<b>51</b>	<b>P-5250 Receipt of Notification of Amendment</b>
<b><u>51</u></b>	<b>P-7000 Accounting for Disclosures</b>
<b>51</b>	<b>P-7100 Maintenance of Records of Disclosures</b>
<b>52</b>	<b>P-7210 Procedure to Request an Accounting of Disclosures</b>
<b><u>52</u></b>	<b>P-7220 Charges for Accountings of Disclosures</b>
<b>52</b>	<b>P-7230 Suspension of a Patient's Right to Receive an Accounting of Disclosures</b>
<b><u>53</u></b>	<b>P-7300 Information to Be Provided in an Accounting of Disclosures</b>
<b>53</b>	<b>P-7400 Documentation of Accountings Provided to Patients</b>
<b>53</b>	<b>P-7500 Documentation of Disclosures Requiring an Accounting</b>
<b>54 - 55</b>	<b>P-7575 Destruction/Disposal of Protected Health Information</b>
<b>55</b>	<b>P-8000 Resolution of Complaints and Breaches</b>
<b><u>56</u></b>	<b>P-8100 Submission of Complaints</b>
<b>56</b>	<b>P-8200 Complaint Resolution Procedures</b>
<b>56</b>	<b>P-8210 Complaints Concerning Privacy Policies and Procedures</b>
<b><u>57</u></b>	<b>P-8220 Complaints Arising From Possible Violation of Privacy Policies</b>
<b><u>58</u></b>	<b>P-8300 Documentation of Complaints</b>
<b>58</b>	<b>P-8400 Mitigation</b>
<b><u>59</u></b>	<b>Red Flag Rules</b>
<b><u>60 - 63</u></b>	<b>Form PF-1000 Notice of Privacy Practices</b>
<b><u>64</u></b>	<b>Form PF-2000 Acknowledgement of Receipt of Notice of Privacy Practices or Attempt to Obtain Acknowledgement</b>
<b><u>65</u></b>	<b>Form PF-3000 Authorization for Use and/or Disclosure of Protected Health Information page 1</b>
<b><u>66</u></b>	<b>Form PF-3000 Authorization for Use and/or Disclosure of Protected Health Information page 2</b>
<b><u>67</u></b>	<b>Form PF-4000 Tracking Log for Disclosure of Protected Health Information</b>

<b><u>68</u></b>	<b>Form PF-5000 AUTHORIZATION TO COMMUNICATE PATIENT'S MEDICAL INFORMATION</b>
<b><u>69</u></b>	<b>Form PF-6000 Certificate of Destruction Form</b>
<b><u>70</u></b>	<b>Form PF-7000 Checklist for verification of patient identity</b>
<b><u>71</u></b>	<b>Form PF-7000 back side (Red Flags)</b>
<b><u>72</u></b>	<b>Form PF-8000 HIPAA Incident Report Form</b>
<b><u>73</u></b>	<b>Information on reporting breach and sample letter</b>
<b><u>74 - 77</u></b>	
<b><u>Index</u></b>	
<b><u>78 - 103</u></b>	<b>Security Policies &amp; Procedures</b>
<b><u>104-105</u></b>	<b>Security Form S1080 &amp; Log</b>

**HIPAA**

**SECURITY**

**POLICIES & PROCEDURES**

**PROHEALTH PARTNERS/**

**ARGUS MEDICAL MANAGEMENT**

## **Introduction to the Security Policy and Procedure Manual**

The purpose of this policy and procedure manual is to establish a comprehensive program to protect the security of sensitive information collected, stored, received, or transmitted by the medical practice.

The medical practice has an obligation under federal law and regulations to:

1. Ensure the confidentiality, integrity, and availability of all protected health information (PHI) it creates, receives, maintains, or transmits in electronic form
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted under the federal privacy regulations

4. Ensure compliance with federal standards and other requirements by its workforce

*Protected health information* includes all individually identifiable health information. The security regulation applies only to PHI that is created, received, transmitted, or stored in electronic form or that is created, received, transmitted, or stored on behalf of the medical practice by a business associate.

The policies and procedures included in this manual apply to all members of the medical practice's *workforce*—including both employees and staff members of the practice. Independent contractors who perform work under the supervision of the medical practice staff are part of the practice's workforce. Consultants or vendors who perform services for the practice but are not under the supervision of practice staff members are considered “business associates” of the practice but not members of the practice's workforce.

## **S-1000 Access Authorization**

### **Policy**

Staff members receive authorization to access PHI and to use the medical practice's workstations, conduct transactions, and run software applications based on their job responsibilities and qualifications. Authorization enables staff members to use the information resources of the practice. Staff members should not access information for other staff members who lack appropriate authorization.

### **Procedures**

Only authorized staff members are allowed to use workstations (computer terminals, personal computers, and other devices) that can access PHI.

A unique user ID and password and specific, assigned static IP address are required to use the medical practice's information system.

## **S-1010 Access Control and Validation Procedures**

### **Policy**

All components of the medical practice's information system are housed in secure locations.

Visitors to the medical practice are accompanied by a staff member when in a position to access the practice's information resources.

Consultants and contractors responsible for installing, maintaining, or testing computer equipment and software are authorized to access the medical practice's information systems in the same manner as though they were staff members authorized to perform similar tasks or functions.

### **Procedures**

Components of the medical practice's information system other than workstations are located in secure, locked areas or cabinets. Only staff members authorized to use or service that equipment have keys to secure areas.

All visitors to the medical practice are to register with the receptionist and sign the visitor log. See Form SF-1010. The visitor log includes:

The name of the visitor

The company or government entity represented by the visitor

The purpose of the visit

The time of arrival

The person being visited

The time the visitor leaves the facility

Visitors to the medical practice are not left alone except in public waiting areas. Visitors should not be left alone in areas such as physician offices in which they may be able to access the practice's information system.

Contractors and maintenance personnel who are not members of the staff sign the visitor's log but need not be accompanied by a staff member at all times when performing work covered by a business associate agreement.

Contractors and maintenance personnel are given a unique user ID and password that enables the practice to monitor their access to the medical practice's information resources. Before a user ID is activated, the security official reviews with the contractor the

### **S-1020 Access Control**

#### **Policy**

The security official ensures that the medical practice's information systems implement technical measures that permit access to the practice's information resources only by those persons who have appropriate authorization.

### **S-1030 Access Establishment and Modification**

#### **Policy**

Implement policies and procedures that, based upon the medical practice's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

The medical practice grants individual users the right to access PHI and related information resources consistent with its access policies and procedures. When a staff member's access authorization needs to be changed, a formal request should be submitted to the security official, who then reviews the request and authorizes the revised access privileges if the request meets the medical practice's authorization requirements.

The ability of staff members and other users to use workstations or computer programs, to conduct specific transactions, or to perform various functions, tasks, or procedures, is determined by the access authorization of each individual. Installation of new software, backing up data, and maintaining and configuring computer hardware or software will only be performed by the assigned Information Systems Technologist(s).

### **S – 1031 Remote Access Control**

Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be explicitly authorized, in writing, by the information owner (physician) or his/her designated representative. If authorized, the organization:

- 1. Authorizes remote access to the information system only to those approved for remote access and only through use of corporate recognized IP address and approved product**

**(GoToMyPC) connecting with host computer using completely private data stream encrypted end-to-end with 128-bit Advanced Encryption Standard (AES).**

- a. Documents allowed methods of remote access to the information system;
- b. Establishes usage restrictions and implementation guidance for each allowed remote access method;
- c. Monitors for unauthorized remote access to the information system;
- e. Enforces requirements for remote connections to the information system.

**Implementation Standard(s)**

This control requires explicit authorization prior to allowing remote access to HIPAA protected information. Remote access is any access to an information system by a authorized user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). A virtual private network (VPN) when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization-controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. **Enforcing access restrictions associated with remote connections is accomplished by control through the Security Systems Officer and IT Security Officer.**

**Assessment Procedure**

Determine if:

There is appropriate prior authorization for the remote access by IP address

There is documentation of allowed methods of remote access to the information system

There are established usage restrictions and implementation guidance for each allowed remote access method.

There is monitoring for unauthorized remote access to the system

There is enforcement for remote connections to the information

**Wireless Access**

The organization prohibits the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the information owner or his/her designated representative. If authorized, the organization:

- a. Monitors for unauthorized wireless access to the information system; and
- b. Enforces requirements for wireless connections to the information system.

**Implementation Standard(s)**

1. If wireless access is explicitly approved, wireless device service set identifier broadcasting is disabled and the following wireless access controls are implemented:

- (a) Encryption protection is enabled;
- (b) Access points are placed in secure areas;
- (c) Access points are shut down when not in use (i.e., nights, weekends);

- (d) A firewall is implemented between the wireless network and the wired infrastructure; **There is to be no remote access allowed to the firewall**
- (e) MAC address authentication is utilized;
- (f) Static IP addresses, not DHCP, is utilized;
- (g) Personal firewalls are utilized on all wireless clients;
- (h) File sharing is disabled on all wireless clients;
- (i) Intrusion detection agents are deployed on the wireless side of the firewall; and
- (j) Wireless activity is monitored and recorded, and the records are reviewed on a regular basis.

## **Guidance**

Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. In certain situations, wireless signals may radiate beyond the confines and control of organization-controlled facilities.

## **Assessment Procedure**

1. the organization establishes usage restrictions and implementation guidance for wireless access;
2. the organization monitors for unauthorized wireless access to the information system;
3. the organization authorizes wireless access to the information system prior to connection;
4. the organization enforces requirements for wireless connections to the information system.
5. the organization meets all the requirements specified in the applicable implementation standard(s).

## **Access Control for Mobile Devices - Staff**

The organization prohibits the connection of portable and mobile devices (e.g., notebook computers, personal digital assistants [PDA], cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) to its information systems unless explicitly authorized, in writing, by the information owner or his/her designated representative. If authorized, the organization:

- a. May employ an approved method of cryptography to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops;
- b. Monitors for unauthorized connections of mobile devices to its information systems;
- c. Enforces requirements for the connection of mobile devices to its information systems;
- d. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;
- e. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and
- f. Protects the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code, virus protection software.

## **Access Control for Mobile Devices – Physician(s)**

Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Usage recommendations and implementation guidance related to mobile devices include, for example,

1. to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls
2. configuration management,
3. device identification and authentication,
4. implementation of mandatory protective software (e.g., malicious code detection, firewall),
5. scanning devices for malicious code,
6. updating virus protection software,
7. scanning for critical software updates and patches,
8. conducting primary operating system (and possibly other resident software) integrity checks, and
9. disabling unnecessary hardware (e.g., wireless, infrared).

Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay.

Policies and procedures recommendations for mobile devices used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.

## **S-1040 Accountability**

### **Policy**

A record is maintained of any movements of computer equipment within the medical practice and all removal of equipment and storage media from the practice.

This policy applies to the transfer of storage media to off-site storage locations.

This policy does not apply to routine shifting of equipment during ordinary operation or maintenance.

### **Procedure**

All computer hardware installed in the medical practice is recorded in a hardware inventory maintained by the assigned Information Systems Technologist(s) who reports to the security official. The log includes:

- \* A description of the equipment
- \* The equipment serial number
- \* The date on which the equipment was installed

- \* The location of the equipment
- \* The name of the person responsible for installation

Log entries are made in the inventory of computer hardware for all equipment that is removed from the medical practice's facilities. The log entry includes:

- \* The date on which the equipment was removed
- \* The destination of the equipment
- \* The reason for removal, such as repair or disposal
- \* The person responsible for preparing the equipment for removal including any sanitizing of storage devices
- \* The date on which the equipment was removed

When storage media are transferred to off-site storage facilities, a record is made of the date and time the media were removed from the facility and the date and time the media arrived at, and were processed, by the storage facility.

## **S-1050 Applications and Data Criticality Analysis**

### **Policy**

As part of the development of a comprehensive contingency plan, the security official assesses the relative criticality of specific applications and data. Arrangements are made to ensure that critical applications and equipment are replaced within one work day in the event of failure. Critical data are backed up as provided in the back-up plan.

### **Procedures**

The security official orders analysis of all applications, computer hardware, and medical practice data to identify those applications, hardware components, and data sets that are critical to the successful operation of the practice. The security official reviews the criticality analysis practice and updates it as needed. The criterion for identifying critical components is whether rendering a component unusable or unavailable would significantly disrupt the practice's ongoing operation. In making this determination, the availability of options for replacing the affected components is assessed. The analysis must identify those components that must be quickly replaced or restored to operating condition during an emergency. It must also identify the longest potential period of time those critical components can be unavailable, and the most cost-effective method of restoring function within the critical time period.

## **S-1060 Assigned Security Responsibility**

### **Policy**

Compliance with federal security standards is the responsibility of the security official.

### **Responsibilities**

The security official is responsible for:

- \* Establishing the medical practice's security program and overseeing its implementation

- \* Ensuring compliance with federal and state security regulations and standards
- \* Reviewing all purchases or acquisitions of information technology for consistency with the medical practice's security policies and standards
- \* Investigating security incidents (i.e., known or suspected violations of security policies and procedures and breaches in security measures or the security of the medical practice's protected health information)
- \* Reviewing information system activity to ensure compliance with the medical practice's security policies and procedures
- \* Developing and implementing a security training and awareness program for the medical practice's employees and staff, including temporary employees.
- \* Reviewing and approving the security provisions of contracts with business associates
- \* Delegating specific tasks such as review of business associate contracts, while remaining responsible for compliance with the medical practice's security policies and standards
- \* Reviewing annually compliance with security requirements, policies, and standards

## **1.Change Management, Information Technology – IT Security Official**

### **Statement of Policy**

To ensure that Practice is tracking changes to networks, systems, and workstations including software releases and software vulnerability patching in information systems that contain electronic protected health information (“ePHI”). Change tracking allows the Information Technology (“IT”) Department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

### **Procedure**

1. The IT staff or other designated Practice employee who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system.
  - a. When changes are tracked within a system, i.e. Windows updates in the Add or Remove Programs component or electronic health record (EHR) updates performed and logged by the vendor, they do not need to be logged on the change management tracking log; however, the employee implementing the change will ensure that the change tracking is available for review if necessary.
2. The employee implementing the change will ensure that all necessary data backups are performed prior to the change.
3. The employee implementing the change shall also be familiar with the rollback process in the event that the change causes an adverse effect within the system and needs to be removed.

General Excel based log. See **Form SF - 1105**

### **S-1070 Audit Controls**

## **Policy**

The security official implements technical measures to create a record of information system activity, including user log-on/log-off and start-up/shut-down of technical security measures.

## **Procedure**

The security official periodically reviews records of system activity to identify security problems and to evaluate compliance with security policies and procedures.

## **S-1080 Authorization/Supervision**

### **Policy**

All employees and other members of the medical practice's workforce must be specifically authorized to use the information resources or to access PHI. Or they must be under the direct supervision of an appropriately authorized staff member when working with PHI or on components of the medical practice's information system. See Form S-1080 for Policy and Procedure for Temporary and/or Float Pool access to information.

### **Procedure**

Generally, staff members are authorized to use only the PHI needed to perform their professional and job responsibilities.

The job description of every staff member should specify the access to information resources and PHI that is authorized. The following categories of access authorization have been established:

## **S-1090 Clinical Authorization**

Physicians, nurses, and other health professionals may access any information contained in a patient's records (other than information that has been restricted by the patient's physician) for the purpose of treating the patient, including consulting with other professionals concerning the patient's treatment.

## **S-1100 Clerical Authorization**

Clerical staff responsible for preparing and submitting claims and processing payment information may access any information contained in a patient's records needed to meet requirements for submission and adjudication of a claim for services.

## **S-1110 Administrative Authorization**

Members of the medical practice's management may access any information contained in patient records when required for the purpose of supervising staff or complying with licensing and other regulatory requirements.

## **S-1120 IT Management Authorization**

Staff responsible for managing the medical practice's information resources may access information needed to configure security features of computer hardware and software. Examples include establishing user passwords and setting permissions to access data or configure hardware and software.

A staff member who requires access to information that he or she is not authorized to access should request the assistance of an appropriately authorized staff member.

Maintenance and housekeeping staff who may have physical access to PHI should be supervised closely enough to reasonably ensure that the security policies of the medical practice are not violated.

Staff members who are authorized to access PHI must complete security and privacy training, and must review the limitations on their access to information and information resources.

### **S-1130 Automatic Log-off**

#### **Policy**

All workstations are configured to log users off 10 minutes of inactivity. After being automatically logged off, a user must re-enter his or her user name and password to resume the interrupted activity.

Users may not disable this automatic log-off feature.

### **S-1140 Business Associate Contracts/Agreements**

**Instruction:** Medical practices must use the current contract/agreement for Business Associates.

#### **Policy**

Business associate agreements must include the following provisions or provisions with an equivalent effect.

#### **Required Provision Guidelines**

##### **S-1150 Implementation of Security Safeguards**

The business associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI that it creates, receives, maintains, or transmits on behalf of the covered entity. These safeguards shall be equivalent or identical to the administrative, physical, and technical safeguards that the covered entity is required to implement under the federal security and privacy regulations.

##### **S-1160 Extension to Agents and Subcontractors**

If the business associate uses an agent or subcontractor to perform any of the work covered under an agreement with the medical practice, and such work involves the creation or use of PHI, the business associate enters into a written contract or agreement with the subcontractor or agent that includes the same safeguards required by the agreement between the medical practice and the contractor.

##### **S-1170 Reporting**

The business associate must be required to report to the medical practice any security incident of which it becomes aware.

##### **S-1180 Contract Termination**

The medical practice may terminate the contract with the business associate if the practice determines that the associate has violated a material term of the contract, including any provisions related to the security and privacy of PHI.

**Note:** This provision may be omitted if the statutory obligations of the medical practice or its business associate make termination of the contract impossible.

### **S-1190 Business Associate Contracts**

#### **Policy**

A business associate that creates, receives, maintains, or transmits electronic PHI for the medical practice must provide satisfactory assurances that it will appropriately safeguard the information. These assurances must be included in a written contract or other arrangement with the business associate.

#### **Procedure**

Written contracts or agreements must be established with all business associates before the exchange or creation of PHI with or by the associate.

All written contracts or agreements must contain the assurances identified in the medical practice's policies for business associate agreements, including the required termination provisions.

### **S-1200 Contingency Operations**

#### **Policy**

Only staff responsible for implementing specific aspects of contingency plans, including maintaining essential services during emergencies and monitoring unsecured areas housing components of the medical practice's information system, are permitted access to facilities during an emergency.

#### **Procedure**

All staff members responsible for implementation of contingency plans have keys, passwords, and other information or devices needed to gain access to information system components during emergencies.

Staff members responsible for implementing contingency plans may take whatever actions they determine necessary to obtain back-up data sets and restore system function.

All actions taken by staff members to restore system functions during an emergency are to be documented and reviewed with the security official upon the conclusion of the emergency.

### **S-1210 Contingency Plan**

#### **Policy**

The security official establishes policies and procedures that protect the security of PHI during an emergency caused by fire, vandalism, system failure, natural disaster, or other contingencies. Security includes the availability, integrity, and confidentiality of the information.

#### **Procedure**

The security official develops a comprehensive contingency plan based on a comprehensive examination of the impact of natural, human, and environmental contingencies on the medical practice's ability to secure its information and information resources.

The contingency plan identifies the major natural and man-made disasters that could adversely affect the availability, integrity, and confidentiality of PHI maintained in electronic form.

The contingency plan identifies the actions that will be taken to compensate for disasters that affect the availability, integrity, and confidentiality of PHI.

The contingency plan assigns specific responsibilities to members of the staff. These responsibilities specifically address failures in normal security safeguards that are likely to occur during an emergency.

The security official reviews, tests, and updates the contingency plan as needed.

### **S-1220 Data Back-up and Storage**

#### **Policy**

Before computer equipment is relocated within or removed from the medical practice's facilities, a back-up copy is created of any information that is contained on storage devices that are integral parts of a piece of computer equipment.

#### **Procedure**

The staff members responsible for maintenance of the computer equipment ensure that a complete back-up data set of any information contained on the computer equipment is made before the equipment is removed from or relocated within the medical practice's facilities.

## **S-1230 Data Back-up Plan**

### **Policy**

The security official develops a comprehensive plan to back up PHI and critical applications, or implements fault-tolerant systems that reduce the likelihood that equipment failure or disasters will adversely affect the integrity and availability of PHI.

### **Procedures**

Detailed back-up procedures are documented in the medical practice's contingency plan. These procedures create an exact copy of PHI at a given point in time. The detailed back-up procedures specify an interval for the creation of back-up data sets.

Back-up copies of PHI are to be stored in a secure but accessible location as specified in the medical practice's contingency plan.

## **S-1240 Disaster Recovery Plan**

### **Policy**

The medical practice maintains back-up data sets that can be used to re-create data lost as a result of machine failure or other disaster.

### **Procedure**

Staff members who believe that a system failure or other disaster has resulted in the loss of information should report the possible failure to the security official or on-duty staff member responsible for operating the information system.

Technical staff members responsible for preparing back-up data sets test the back-up copies to ensure that they:

- \* Contain an exact copy of the information they back up
- \* Can be restored when needed

The security official determines when a back-up data set should be used to re-create or restore lost data. Procedures for restoring data are documented in the contingency plan.

Staff members are notified of any data that are lost following restoration of the back-up data set. For example, a machine failure has destroyed information created since the last back-up. Staff members should be notified that these data have been lost.

Back-up copies should be made available to users within one working day of being requested.

## **S-1250 Disposal**

### **Policy**

All electronic media—such as fixed and removable disk drives, rewritable CD-ROMs, and back-up tapes that are used to store PHI or information enabling security features of the practice's information systems—are “sanitized” using the following procedure.

Before sale or disposal, all computer hardware is examined and certified as containing no PHI or information enabling security features of the medical practice's information system, including information that would enable a user to access the practice's information system.

### **Procedure**

All storage devices and media are to be given to the security official for disposal. Storage devices and media may be disposed of only by an authorized staff member.

Prior to disposal, the storage media are sanitized either by means of degaussing, triple overwriting, or physically dismantling and destroying the storage media.

All CD-ROMs, including rewritable CD-ROMS, are rendered unreadable by abrading the data storage surface before disposal.

All software and data are removed from all computer equipment prior to sale or disposal of the equipment. Disk drives are sanitized by degaussing or triple overwriting.

Logs are maintained of all computer equipment and storage media that have been disposed of. These logs include the date on which storage media were sanitized and a description of the sanitizing method used.

## **S-1260 Emergency Access Procedure**

### **Policy**

The medical practice's computer equipment is configured to allow only staff members with appropriate authorization to access information stored on the computer and to configure software installed on the equipment.

Staff members responsible for implementing contingency plans must have authorization that enables them to repair equipment and implement emergency procedures.

If user accounts must be deleted or disabled to repair equipment failures or restore functions during an emergency, the affected users are notified and new user names and passwords are established.

### **Procedure**

A written record of so-called "administrator" user account names and passwords is maintained by the security official in a secure, locked file. An administrator user account is an account that has full authorization to configure equipment and software.

## **S-1270 Emergency-mode Operation Plan**

### **Policy**

The medical practice has established procedures to safeguard the security of PHI during emergencies that impair normal security safeguards. The staff members responsible for creating and implementing these procedures are specified in greater detail in the medical practice's contingency plan.

### **Procedure**

The security official develops detailed emergency-mode operating procedures as part of the comprehensive contingency plan. These procedures safeguard the medical practice's information resources and PHI during emergencies that disrupt normal security measures.

During an emergency that disrupts power supplies, the medical practice's information systems are shut down. Only the following are supported by back-up power supplies or alternative power sources:

Network offsite servers

Power interruptions and other disasters that disrupt even these essential services are sufficient reason to close the medical practice until essential services have been restored. Patients requiring emergency treatment will receive stabilizing treatment and be transferred to a facility where adequate care can be provided.

During power disruptions, staff members maintain paper records of information that would ordinarily be recorded electronically. After restoration of power, electronic databases are updated from these paper records.

When an emergency condition exposes components of the medical practice's information system to theft or unauthorized removal, the security official or a designated staff member is present to prevent loss of information or essential system components. A complete inventory of any damage to information system components is conducted after the resolution of the emergency condition.

## **S-1280 Encryption and Decryption**

### **Policy**

When determined necessary by the security official, information transmitted outside the practice is encrypted to prevent use by unauthorized individuals.

### **S-1281 Guidelines**

Data should be encrypted when it is transmitted over a network that might be accessible by unauthorized individuals. Information that can be used to alter or defeat the medical practice's security measures also should be encrypted.

The technical methods used to implement encryption and decryption are determined by the security official.

## **S-1290 Encryption**

### **Policy**

The security official identifies any circumstances under which information transmitted by the practice must be encrypted to prevent its use by unauthorized recipients.

The security official ensures that staff members responsible for transmitting information are familiar with encryption requirements and the use of encryption software.

Staff responsible for transmitting information must encrypt it when directed to do so by the security official.

### **S-1300 Evaluation**

#### **Policy**

Comprehensive evaluations of the technical and non-technical components of the medical practice's information systems are conducted by the security official to document compliance with federal and state security standards and to identify areas of noncompliance. Based on these evaluations, the security official develops and implements action plans to bring the practice into compliance with federal and state security regulations and standards.

#### **Procedure**

The security official prepares the evaluation using all necessary internal and external resources.

The security official prepares a comprehensive report documenting the findings of the evaluation and compliance action plan.

The evaluation report is presented to the medical practice's management for approval.

### **S-1310 Access Controls**

#### **Policy**

The security official develops and implements policies and procedures that allow only authorized staff members and contractors to physically access the medical practice's electronic information systems. The areas of the practice's facilities in which components of its information systems are housed are physically secure and deny access to all but properly authorized staff members. See Security Form SF – 1100 Facility Access Control Log to track all outside access.

### **S-1320 Facility Security Plan**

#### **Policy**

All computer equipment and devices that are used to access, transmit, or store PHI are protected from unauthorized physical access, tampering, and theft.

#### **Procedure**

Network servers and storage devices are housed in a secure location that cannot be accessed by visitors to the practice. The equipment closet, office, or room in which such equipment is located is locked at all times.

Back-up copies of PHI are stored in a secure location. Back-up media stored on-site are kept in locked cabinets. Back-up media stored off-site are stored in a manner that prevents physical access by anyone lacking proper authorization.

### **S-1330 Information Access Management**

#### **Policy**

The security official is responsible for developing and implementing procedures to authorize staff members' use of the medical practice's information resources. This includes establishing access to PHI, based on the staff member's job responsibilities and qualifications. Authorization is limited to the information the individual needs to fulfill his or her job responsibilities.

### **S-1340 Information System Activity Review**

#### **Policy**

The security official periodically reviews records of information system activity, such as audit logs, access reports, and security incident tracking reports.

#### **Procedure**

The security official reviews all security incidents reports and ensures that any breaches in security have been corrected.

The security official regularly reviews records of system activity to identify any patterns of activity that suggest the medical practice's security policies and procedures have been breached, either by members of its workforce or by individuals or organizations that are not business associates of the practice. The security official determines whether security has been violated and takes appropriate corrective action, including changes in security policies and procedures.

The security official maintains records of all reviews of security incidents and system activity, and reports any findings to other members of the medical practice's management.

### **S-1350 Integrity Controls**

#### **Policy**

Applications that transmit information electronically must include technical capabilities to ensure that the information received by the recipient is the information that was transmitted.

### **S-1360 Integrity**

#### **Policy**

The security official implements procedures and technical measures to guard electronic health information from improper alteration or destruction. Staff members must follow these procedures and may not take any action to evade the technical measures.

### **S-1361 Guidelines**

The technical measures implemented by the security official should permit modification of PHI only by staff members with appropriate authorization.

Applications used to create and modify PHI should support tracking of changes to records including the identity of the staff member making the change, the nature of the change being made, and the date on which the change was made.

**Note:** These mechanisms are intended to mimic the tracking that can be performed using paper records. That is, when a paper record is modified, the staff member making the change ordinarily identifies the information being changed, notes the change, and initials or signs and dates the modification. When making such changes in an electronic version of the same record it would be impossible to track changes—or even to identify that a change had been made—unless the application includes features that enable such tracking.

### **S-1370 Isolating Health Care Clearinghouse Functions**

**Note:** This policy is needed only if the medical practice provides health care clearinghouse services for other medical practices or covered entities.

#### **Policy**

PHI processed on behalf of other medical practices is isolated from PHI related to the patients of the practice.

Information related to the medical practice's patients and the patients of clearinghouse clients is not commingled. Only those staff members responsible for administration of the clearinghouse functions are authorized to access PHI for clearinghouse clients.

### **S-1380 Log-in Monitoring**

#### **Policy**

Log-in procedures limit the number of unsuccessful log-in attempts to four, after which a user must contact the information system administrator to have his or her password reset.

The security official reviews log-in monitoring records and investigates patterns that suggest the possibility of security breaches or attempted penetration of security measures by unauthorized users.

#### **Procedure**

Operating systems are configured to monitor log-in attempts.

The security official maintains a record of any investigations of suspected efforts to penetrate security measures by unauthorized users.

### **S-1390 Maintenance Records**

## **Policy**

All repairs and modifications to the physical components of the medical practice's facilities that are related to security (hardware, walls, doors, and locks, for example) are documented in the practice's risk-assessment and risk-management plan. (See form SF – 1100)

## **Procedure**

The security official must approve in advance any modifications to the physical facilities housing components of the medical practice's information system.

The security official will make needed changes to the risk-assessment and risk-management plan that reflect these changes in physical facilities.

## **S-1400 Media Re-use**

### **Policy**

All storage media, including removable disks, rewritable CD-ROMs, and back-up tapes, are "sanitized" before re-use.

### **Procedure**

Before re-use, storage media are "sanitized" either by means of degaussing or triple overwriting.

## **S-1410 Password Management**

### **Policy**

All users must select a password conforming to the following guidelines:

- \* Passwords should be between 8 and 10 characters except for all privileged users should be minimum 14 and complex and changed every 60 days.
- \* Passwords should not be the name of a pet, spouse, child, or parent.
- \* Passwords should be a word or sequence of letters and numbers that the user can remember but could not be easily guessed by even a close friend of the user.
- \* Passwords should never be written down.
- \* Passwords should never be given to other staff members.
- \* A new password should be selected every three months, 60 days for privileged users, and current or previous passwords should not be re-used.

### **Procedure**

The security official reviews password policies when a user first receives his or her user ID.

The security official monitors password usage and identifies any patterns that suggest password policies and guidelines are not being followed.

The security official requires staff members who frequently lose or forget their passwords to complete retraining on the correct use of passwords.

## **S-1420 Person or Entity Authentication**

### **Policy**

All users must use their passwords when logging on to the medical practice's information system. Passwords should not be written down or disclosed to other members of the staff, friends, family, or anyone else.

A staff member may not use another staff member's user name and password to access the medical practice's information system. Staff members may not give their passwords to other staff members.

Passwords should comply with the following guidelines.

### **S-1421 Guidelines**

Passwords should consist of between eight and 10 characters.

Users should not select as a password any word that can be easily guessed such as:

- \* The name of a child
- \* A pet
- \* A favorite sports team
- \* A school he or she has attended
- \* A hobby
- \* Any other information that a person who knows the user might guess

Users must change their passwords once they become known to others.

Users should change their passwords at least once every year, but not so frequently that they are likely to be forgotten.

### **S-1430 Protection from Malicious Software**

#### **Policy**

Anti-virus software is installed on all computer workstations and servers to protect the medical practice and its information from attack by malicious software such as computer viruses, worms, and Trojan horses.

#### **Procedure**

The security official is responsible for ensuring that anti-virus software has been installed on all workstations and on network servers. The security official also ensures that anti-virus software is regularly updated.

Staff members must not disable anti-virus software and must immediately take action to report virus infections and remove viruses from affected machines when the anti-virus software identifies an infection. The security official maintains a log of virus infections and detections that includes a record of successful eradication of viruses and cleaning of affected files and computer applications. Staff members are responsible for reporting all viruses detected by anti-virus software. The security official confirms that the viruses have been successfully removed from the affected machines.

Staff members with access to the Internet should not open e-mail messages and e-mail attachments from unknown senders.

### **S-1440 Risk Analysis**

#### **Policy**

The security official conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by the covered entity.

#### **Procedure**

A comprehensive analysis of security threats is reviewed and updated as needed.

The risk analysis comprehensively describes the medical practice's information system, including the following components:

- \* The computer hardware and software that make up the medical practice's information system
- \* The categories and qualifications of staff members who use the system
- \* The functions and activities that are supported by the information system
- \* The data and information that are collected, processed, and stored by the information system
- \* The physical environment that houses information system components
- \* On-site and off-site storage of information
- \* The organizations to which information is transmitted
- \* The data and information that are transmitted to other organizations

- \* The internal and external connections between the medical practice's information system and the information systems of other organizations

The risk analysis identifies threats to the security of the medical practice's PHI, including natural, human, and environmental threats. The risk analysis identifies the nature of each threat or vulnerability and how each may damage information security.

The risk analysis indicates the preventive measures that the medical practice has implemented (or is planning to implement) to limit the damage that might be caused by each threat or vulnerability.

The risk analysis evaluates the likelihood that each security threat or vulnerability might occur.

The risk analysis describes the nature and extent of the damage each threat might cause to the integrity, availability, and confidentiality of the medical practice's information resources.

The risk analysis identifies high-priority threats that are the focus of risk-management efforts.

The risk analysis recommends controls or actions to lessen the risk associated with high-priority threats.

The risk analysis is reviewed and approved by the security official. The results of the risk analysis are shared with other members of the medical practice management team and presented to the governing body of the practice.

### **S-1450 Risk Management**

#### **Policy**

The security official implements a comprehensive risk-management program based on the results of the risk analysis. The risk-management program includes the security measures identified by the risk analysis. The purpose of these security measures is to reduce risks and vulnerabilities to a reasonable and appropriate level.

#### **Procedure**

The security official develops a comprehensive risk-management plan. The security official reviews the risk-management plan and updates it as needed.

The risk-management plan summarizes the results of the risk analysis, including the major security threats the risk-management plan addresses and the measures that will be implemented to mitigate or reduce risks to an acceptable level.

The risk-management plan identifies the specific actions that will be taken to implement the security measures identified in the risk analysis, including a timetable for implementation of each measure.

The risk-management plan clearly describes the magnitude of the risks that will be accepted if the plan is adopted. The plan must include documentation that the accepted risks are reasonable based on the unavailability of cost-effective risk reduction measures. Risks are considered reasonable if they cannot be reduced, can only be reduced by adopting measures that would severely impair the ability of the information system to perform its intended functions, or can be reduced only by implementing measures whose cost substantially exceeds the anticipated costs of any security failures that would be prevented.

The risk-management plan is reviewed with and approved by the governing body of the medical practice annually.

### **S-1460 Sanction Policy**

#### **Policy**

Employees and other members of the medical practice's workforce are subject to sanctions for violating the medical practice's security policies and procedures.

#### **Procedure**

Violations of security measures and the penalties associated with them include the following.

### **S-1470 Minor Security Breaches**

This category of breaches consists of minor or unrepeatable violations of security policies.

*Sanction:* A minor infraction such as this will result in brief counseling and, if necessary, additional security training.

*Example:* A staff member briefly leaves her workstation unattended without logging off to prevent injury to a patient or another staff member or due to sudden illness.

### **S-1480 Significant Security Breaches**

This category includes any documented violation of the security of PHI that could easily have been avoided had the staff member exercised due care.

*Sanction:* A pattern of repeated, significant violations of security policy may be grounds for temporarily suspending an employee and may lead to termination of the employee.

*Example:* A staff member attaches a note to his workstation monitor that gives his user ID and password.

### **S-1490 Severe Security Breaches**

This category includes any deliberate violation of security policies and procedures or confidentiality requirements that are not justified by considerations of employee or patient health and safety or were not necessary or unavoidable during an emergency situation.

*Sanction:* A deliberate violation of security policies will result in the immediate suspension of the employee or other workforce member and the termination of all access to protected health information and information resources.

*Example:* A staff member makes a copy of PHI and gives it to a vendor without obtaining required authorizations.

It is the responsibility of an employee's supervisor to identify security breaches and apply appropriate sanctions.

An employee or other workforce member who believes that he or she has been wrongly charged with a security violation may appeal the imposition of sanctions to the security official.

### **S-1500 Security Awareness and Training**

#### **Policy**

The security official is responsible for developing and implementing a security awareness and training program for all members of the medical practice's workforce, including professional staff, practice partners, and management.

The training program covers:

- \* The definition of security (availability, integrity, confidentiality)
- \* Threats to security (natural, human, and environmental)
- \* Methods of safeguarding security
- \* Security features of the medical practice's information system and applications
- \* Use of major applications
- \* Policies on installation and configuration of software
- \* Controls on access to information
- \* Correct use of anti-virus software
- \* Contingency plans and disaster procedures
- \* Workstation policies
- \* Good security practices (workstation use policies)
- \* Security incident reporting procedures
- \* User ID and password policies

All staff members, including management and professional staff, are required to complete security training before they can use the medical practice's information systems or are permitted to access PHI.

## **Procedures**

New staff members receive security training as part of their orientation.

Contractors and consultants receive training and/or information on the medical practice's security policies and procedures.

## **S-1510 Security Incident Procedures**

### **Policy**

Security incidents are to be reported promptly to the security official. Incidents should be reported by the staff members responsible for the incident or staff members who identify the incident.

No sanction or penalty is imposed for simply reporting a security incident.

### **Procedure**

The security official investigates security incidents and determines:

1. Whether a breach of security has occurred
2. The appropriate actions to take to repair any damage or potential damage to security that the incident might have caused

The security official ensures that actions needed to repair any damage caused or potentially caused by a security incident are taken.

The security official documents the report of a security incident, the findings of the investigation, and any actions taken in response to those findings.

In the event there is a breach of PHI, these guidelines/regulations from CMS must be initiated and the Company must be notified immediately but no later than 30 days after the first date the breach is discovered:

Written notification shall be provided in concise, conspicuous, plain language that includes the following elements:

- A brief description of what happened, including the date(s) of the breach and of its discovery;
- To the extent possible, a description of the types of personal information involved in the breach (e.g., full name, social security number, date of birth, home address, account number, disability code, etc.);
- A statement whether the information was encrypted or protected by other means, when determined such information would be beneficial and would not compromise system security;
- What steps individuals should take to protect themselves from potential harm, if any;
- What Contractor is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches;

and

- Who affected individuals should contact for more information, including a toll-free telephone number, e-mail address, and postal address.

## **S-1520 Security Reminders**

### **Policy**

The medical practice publishes periodic notices and security updates to maintain awareness of security procedures and sound security practices. Notices are prepared whenever significant new security threats are identified, whenever security features of computer hardware and software are revised or updated, and whenever the security official believes that a security incident warrants calling the attention of staff members to security policies and procedures.

#### **Procedure**

The security official is responsible for preparing, distributing, and posting security notices and periodic updates.

The security official is responsible for announcing the availability of security updates and changes to security policies and procedures at staff meetings.

#### **S-1530 Termination Procedures**

##### **Policy**

A staff member's authorization to use information resources and to access PHI ends upon termination of employment.

##### **Procedures**

Staff members must turn in keys or key cards that give access to computer equipment or facilities upon termination of their relationship with the medical practice.

The security official should be notified of the effective date of any employee termination or of the date on which a staff member's authorization to use the medical practice's information resources will terminate.

The staff member's user account on the medical practice's information system will be disabled or deleted **within 24 hours** upon termination of the relationship with the medical practice.

The staff member will surrender any protected information, including information contained on storage media (e.g., a CD-ROM or removable disk, data storage key, etc.) that may be in the staff member's possession at the time the relationship with the medical practice ends.

The employee should be escorted out of the building and the employee's access authorization should be terminated immediately when the employee's supervisor feels these actions are appropriate to safeguard the security of the medical practice's PHI and information system. The security official should be notified and steps taken to safeguard security such as re-keying locks.

#### **S-1540 Testing and Revision Procedures**

##### **Policy**

Contingency plans are to be reviewed with staff members, tested, evaluated, and revised as necessary at least once every 12 months.

##### **Procedure**

The security official reviews contingency plans with all staff members to ensure that staff members responsible for implementation of contingency plans are appropriately trained.

New staff members are thoroughly trained in contingency procedures when assuming a position that includes responsibilities for implementing contingency procedures.

Back-up data sets are tested to verify that they contain exact copies of the information that they back up and that the back-up data can be successfully restored.

Emergency power supplies are inspected and tested monthly or more frequently to confirm their ability to provide power for the time period specified in the medical practice's contingency plan.

Fire alarms and fire-suppression equipment are inspected and tested every six months, or according to a schedule required by life-safety codes, to confirm that they will operate as intended and be available when needed.

#### **S-1550 Transmission Security**

##### **Policy**

The security official implements technical measures to guard against unauthorized access to PHI that is being transmitted over an electronic communications network.

Staff members responsible for transmitting information must use these measures.

## **S-1560 Unique User Identification**

### **Policy**

Every staff member authorized to use the medical practice's information systems is given a unique user name and selects a password known only to the staff member. Staff members must use their user name and password when using the information system and accessing PHI.

## **S-1570 Workforce Clearance**

### **Policy**

A staff member will be authorized to access PHI and to use information resources if:

1. They meet the minimum professional or technical qualifications for the position they occupy
2. They have not been disciplined for serious infractions of security in previous jobs

Staff members who have been disciplined for infractions of security policies and procedures may be granted restricted access until their trustworthiness has been established to the satisfaction of the security official.

### **Procedure**

When verifying credentials and checking references, the staff member responsible for hiring should determine that the candidate has not been sanctioned or disciplined for infractions of security policies or standards in the past. The Office Of Inspector General "OIG" expects companies like Argus Medical Management to regularly check the "Exclusion" list for the physicians, employees, volunteers and entities with which we do business. Argus is committed to comply with this requirement; therefore, all persons who have access to Protected Health Information (PHI) are subjected to the OIG Compliance provision. There will be an initial & ongoing OIG search of all Argus and ProHealth employees to identify "Sanctioned/Excluded" on the list. The verification of this process may result in disciplinary action up to and including termination of access and/or employment. The Office of Inspector General maintains a list of excluded individuals/entities accessible on the World Wide Web at [www.hhs.gov/oig/cumsan/index.htm](http://www.hhs.gov/oig/cumsan/index.htm) and urges health care providers to check the list before hiring or contracting with individuals or entities. Additionally, the Office of Inspector General recommends that health care providers periodically check the list to determine the exclusion status of current employees and contractors. Employees will sign an authorization form for the initial and ongoing searches.

Any restrictions on access to information resources should be communicated to the security officer so the necessary technical restrictions in access privileges can be implemented.

## **S-1580 Workforce Security Policy**

The security official develops and implements policies allowing only those workforce members who have the appropriate qualifications and job responsibilities to use the medical practice's PHI and information systems.

### **S-1590 Workstation Use Policy**

Users must observe the guidelines on use of workstations:

#### **S-1591 Guidelines All Workstations**

All users must log off all workstations rather than leaving them unattended. This includes workstations in private offices.

Screens should be positioned within workstations so that they are visible only to the persons who use them.

#### **S-1592 Workstations Located in Private Offices**

A workstation in a physician's office is an example of this type of workstation.

These workstations may be used to access all patient information, including both clinical information and billing information and to perform administrative functions related to computer security.

Staff members should not access patient information when visitors to the medical practice, including patients, can view the information that is displayed on a screen.

#### **S-1593 Workstations Located in Common but Non-Public Areas**

A workstation at a nursing station is an example of this type of workstation.

These workstations may be used to access all patient information, including both clinical information and billing information.

Staff members should not access patient information when patients and other visitors to the practice can view the information displayed on a screen.

These workstations should *not* be used to perform administrative functions related to security, such as adjusting settings to enable access to programs or data.

#### **S-1594 System Management Workstations**

A workstation in an office housing a network server or storage is an example of this type of workstation.

These workstations may be used to access all patient information, including both clinical information and billing information. However, patient information should be accessed from these workstations only when necessary to perform maintenance on, or to troubleshoot, the information system.

#### **T-1000 Use of Standard Transactions**

All of the following transactions, when conducted electronically, will be conducted in compliance with the federal standards for electronic transactions.

- claim submission
- claim status request
- remittance advice and electronic fund transfer
- coordination of benefits determination
- eligibility and enrollment determination
- referral authorization
- health plan enrollment
- health plan premium payment

### *Regulation*

---

#### **45 CFR 162.923**

Requires use of federal standards when transactions are conducted electronically.

#### **T-1110 Transaction Standard for Claim Submission and Coordination of Benefits**

ASC X12N 837—Health Care Claim: Institutional,  
Version 4010 (004010X096)

ASC X12N 837—Health Care Claim: Professional,

ASC X12N 837—Health Care Claim: Dental,

NCPDP Batch Standard, Version 1 Release 0

*Regulation*

---

**45 CFR 162.1102**

Establishes federal standard for claims transaction.

**45 CFR 162.1802**

Establishes federal standard for claims transaction.

**T-1120 Transaction Standard for Claims Status Inquiries**

ASC X12N 276/277—Health Care Claim Status Request and Response,  
Version 4010 (004010X093)

*Regulation*

---

**45 CFR 162.1402**

Establishes federal standard for claims status transaction.

**T-1130 Transaction Standard for Remittance Advice and Electronic Funds Transfer**

ASC X12N 835—Health Care Claim Payment/Advice,  
Version 4010 (004010X091)

NCPDP Telecommunications Standard Format,  
Version 5 Release 1

NCPDP Batch Standard, Version 1 Release 0

*Regulation*

---

**45 CFR 162.1602**

Establishes federal standard for remittance advice and electronic funds transfer transaction.

**T-1140 Transaction Standard for Referral Authorization**

ASC X12N 278—Health Care Services Review Information,  
Version 4010 (004010X094)

## Regulation

---

### 45 CFR 162.1302

Establishes federal standard for referral authorization transaction.

### **T-1150 Transaction Standard for Eligibility Transactions**

ASC X12N 270—Health Care Eligibility Benefit Inquiry and Response,  
Version 4010 (004010X092)

NCPDP Telecommunications Standard Format,  
Version 5 Release 1

NCPDP Batch Standard, Version 1 Release 0

## Regulation

---

### 45 CFR 162.1202

Establishes federal standard for eligibility transaction.

### **T-1160 Transaction Standard for Health Plan Enrollment**

ASC X12 834—Benefit Enrollment and Maintenance,  
Version 4010 (004010X095)

## Regulation

---

### 45 CFR 162.1502

Establishes federal standard for enrollment transaction.

### **T-2000 Trading Partner Agreements**

All contracts or agreements with trading partners will include the provisions that comply with federal regulation for *trading partner agreements*. These provisions:

- describe the duties and obligations of both parties to the agreement, including any responsibilities for safeguarding the security and privacy of the information that the two parties exchange
- require electronic transactions to be conducted in compliance with the federal standards for electronic transactions;
- prohibit any addition or modification of the data elements to a standard transaction
- prohibit any use of codes that are not specified in a federal standard transaction code set

- may specify processing instructions for completing transactions between a provider and a third party payer such as specific codes that, if present, will result in the rejection of the transaction.

### *Regulation*

---

#### **45 CFR 162.915**

Establishes federal requirements for trading partner agreements.

#### **T-3000      Updating Code Sets and Practices**

Staff members responsible for coding claims will use only codes contained in the federal transaction standard code sets. Staff will update code sets when new codes are issued.

### *Regulation*

---

#### **45 CFR 162.1000**

Requires use of federal standard code sets.

### *T-3100Diagnosis Coding*

---

Diagnoses must be coded using the International Classification of Diseases, 9th Revision, Clinical Modification (ICD-9-CM Diagnosis Codes)

### *Regulation*

---

#### **45 CFR 162.1002**

Establishes federal standard code sets.

### *T-3200Physician Services Coding*

---

Physician services and surgical procedures must be coded using the Common Procedure Terminology, 4th Revision (CPT-4)

### *Regulation*

---

#### **45 CFR 162.1002**

Establishes federal standard code sets.

### *T-3300Dental Services Coding*

---

Dental services must be coded using the Code on Dental Procedures and Nomenclature (CDT)

*Regulation*

---

**45 CFR 162.1002**

Establishes federal standard code sets.

*T-3400 Other Health-related Services Coding*

---

Most other health-related services must be coded using the Health Care Financing Administration Common Procedure Coding System (HCPCS Level II); and,

*Regulation*

---

**45 CFR 162.1002**

Establishes federal standard code sets.

*T-3500 Drug Coding*

---

Drugs must be coded using the National Drug Code.

*Regulation*

---

**45 CFR 162.1002**

Establishes federal standard code sets.

**FOLLOWING PAGES ARE HIPAA SECURITY FORMS**

**HIPAA Form SF1010**

**Non-Patient  
Visitors**

**PLEASE SIGN IN BELOW**

NON patient Visitors (Pharmaceutical Representatives, Medical Equipment sales, etc.)		
Today's Date _____		
1. The name of the visitor: _____	Company represented: _____	The time of arrival: _____
The purpose of the visit: _____	The person being visited: _____	Time visitor leaves facility: _____
Today's Date _____		
2. The name of the visitor: _____	Company represented: _____	The time of arrival: _____
The purpose of the visit: _____	The person being visited: _____	Time visitor leaves facility: _____
Today's Date _____		
3. The name of the visitor: _____	Company represented: _____	The time of arrival: _____
The purpose of the visit: _____	The person being visited: _____	Time visitor leaves facility: _____

**Form SF-1080**

**TEMPORARY AND/OR FLOAT POOL**

**ACCESS TO PATIENT INFORMATION**

**CARETRACKER LOG IN POLICY AND PROCEDURE**

## Policy for Office Manager, Supervisor or Regional Manager

**Purpose:** To protect the medical information of our patients we need to be able to track who is given what access to the information, when and where.

1. Contact the Help Desk and ask for a Temporary Log In for the Float/Temp.
2. Inform the Help Desk what access the Temp will need, i.e. Demos, Med Records (no MD financial information)
3. **You** assign the Log In and Password, always using the same format: For example: Your office name, the Temp/float's first name and the last 4 digits of the employee's social security number "LPCJane3333" or "DLRDolanJane3333". Ask the float/temp or HR for the Temp's Social Security last four digits.
4. Keep a log of your Temps/Floats (see attached) so that if a privacy or security breach is discovered, we will be able to trace it back to the employee if applicable.
5. When the Temp/Float has completed their assignment in your office, notify the Help Desk to terminate their access.

### **FORM SF-1080 PART 2**

#### **LOG OF TEMPORARY / FLOAT EMPLOYEE ACCESS TO PATIENT INFORMATION**

START DATE: \_\_\_\_\_ EMPLOYEE NAME: \_\_\_\_\_ END DATE: \_\_\_\_\_

START DATE: \_\_\_\_\_ EMPLOYEE NAME: \_\_\_\_\_ END DATE: \_\_\_\_\_



**STAFF NAME COMPLETING REPORT:** \_\_\_\_\_

**STAFF NAME(S) INVOLVED IN INCIDENT:**  
\_\_\_\_\_

**NATURE OF INCIDENT:**  Viewed unauthorized patient data  Altered unauthorized data  
 Copied/Downloaded unauthorized data  Other, please explain any of these incidents in detail below.

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**CONSEQUENCE OF THE ERROR:** (i.e. patient information altered needs correction, stolen, sold, etc.)

\_\_\_\_\_  
\_\_\_\_\_

**CORRECTIVE ACTION / SANCTION PLAN:** *(Work with HIPAA Privacy Officer to develop plan to prevent recurrence)*

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**CORRECTIVE ACTION TIMEFRAME:**  Immediately  One Week  Two Weeks  One Month

**DATE FOR COMPLETION:** \_\_\_\_\_ **DATE COMPLETED:** \_\_\_\_\_

**A COPY OF THIS REPORT SHOULD BE SENT TO: the PHYSICIAN, the REGIONAL MANAGER, the PRIVACY OFFICER, and the SYSTEMS MANAGEMENT SECURITY OFFICER**







# HIPAA FORM SF – 1110 - A

## ATTESTATION OF HIPAA PRIVACY AND SECURITY TRAINING

I hereby attest that I have completed the HIPAA Privacy and Security training provided by Argus Medical Management on the \_\_\_\_\_ day of \_\_\_\_\_, 201\_\_\_\_.  
Date Month Year

I agree to comply with the HIPAA Privacy Rule and related policies and procedures, applicable to my job. This will be expected as part of my continued employment or association. This Attestation is not an assurance of continued employment or association.

I understand that I will have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) and that I must follow the policies and procedures to protect PHI and EPHI. I further understand that there are formal sanctions in place for intentional violation of privacy policies and that the intentional violation of privacy policies and procedures may result in immediate suspension, pending further investigation and termination as well as possible civil and criminal prosecution including fines and imprisonment.

I understand that there will be no retaliation if I witness or become aware of and report suspected violations to law enforcement or to the Office of Inspector General.

I have read and understand the policies, as well as my reporting obligations. There will be refresher training annually and there may be updates or changes that I will be expected to review as they are presented. I understand that if I have any questions about the training, the policies, or any of the information provided to me, that I may contact the Privacy Officer or any of the Security Officers.

NAME (Please Print)

SIGNATURE

DATE

**Note:** Original of this acknowledgement should be maintained in each employee's personnel file, copy emailed to [compliance@prohealthpartners.com](mailto:compliance@prohealthpartners.com)





SF – 1110-C

### ATTESTATION OF HIPAA PRIVACY AND SECURITY TRAINING

I hereby attest that the following staff have completed the HIPAA Privacy and Security training provided by Argus Medical Management for all of 20\_\_:

STAFF TRAINED IN 20\_\_

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

The above have agreed to comply with the HIPAA Privacy Rule and related policies and procedures, applicable to their job. This will be expected as part of continued employment or association. This training and Attestation is not an assurance of continued employment or association.

It is understood that staff will have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) and that they must follow the policies and procedures to protect PHI and EPHI. It is further understood that there are formal sanctions in place for intentional violation of privacy policies and that the intentional violation of privacy policies and procedures may result in immediate suspension, pending further investigation and termination as well as possible civil and criminal prosecution including fines and imprisonment.

It is understood by all above that there will be no retaliation if staff witness or become aware of and report suspected violations to law enforcement or to the Office of Inspector General.

Staff have read and understand the policies, as well as reporting obligations. There will be refresher training annually and there may be updates or changes that staff will be expected to review as they are presented. It is understood that if there are any questions about the training, the policies, or any of the information provided, that staff may contact the Privacy Officer or any of the Security Officers.

NAME (Please Print)	SIGNATURE	DATE
---------------------	-----------	------

**Note:** Original of this acknowledgement should be maintained in HIPAA manual at this location, copy emailed to [compliance@prohealthpartners.com](mailto:compliance@prohealthpartners.com)



SF – 1115



## Authorized Disclosure Tracking Log Form

*This log provides tracking of disclosure of protected health information to authorized entities for purposes of treatment, payment or operations.*

Date Received	Name of Requestor*	Address* (if known)	Purpose*	PHI Disclosed*	Pursuant to:	Date Disclosed*	Disclosed By	Method of disclosure	Method of transfer
				Attach list of multiple patients					

\* Fields required by HIPAA privacy standards

**Key:**

<i>Date Received: The date request is received to disclose or release information when applicable</i>
<i>Name of requestor: Name of entity of person requesting information to be disclosed or released</i>
<i>Address: The address of the entity or person requesting information be disclosed or released</i>
<i>Purpose: A brief description of the purpose of the disclosure to reasonable inform the individual of the basis of the disclosure.</i>
<i>PHI disclosed: A brief description of the information disclosed/released</i>
<i>Pursuant to: identify waiver of authorization, law or public health purpose</i>
<i>Date disclosed: Date the information was released or disclosed</i>
<i>Disclosed by: Staff member processing the request and disclosing the information:</i>
<i>Method of Disclosure: Paper records, CD, flash drive, etc.</i>
<i>Method of Transfer: Picked up by requestor, etc.</i>

Name of person who received the PHI:	
--------------------------------------	--

Signature:	
------------	--

Date PHI Received:	
--------------------	--