# 1200 – HIPAA Policy

## Pro Policy 1200.1

Policy 1: Policy on HIPAA Risk Analysis

### Purpose

PRO is responsible, under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), to ensure the privacy and security of all protected health information ("PHI") that we use or disclose. The foundation of compliance with the HIPAA is the completion of a "Risk Analysis" to identify existing risks and vulnerabilities in the way we create, receive, maintain or transmit our PHI. This policy describes our general approach to our HIPAA Risk Analysis.

### Scope

PRO's HIPAA Risk Analysis includes an assessment of potential risks and vulnerabilities to the confidentiality, availability and integrity of all PHI that PRO creates, receives, maintains or transmits. This includes assessing any risks and vulnerabilities to the confidentiality, integrity and availability of non-electronic PHI (such as papers and documents) and electronic protected health information (e-PHI). At a minimum, the risk analysis will include a review of PRO's:

- General security hardware and procedures to protect our facility, vehicles, and electronic assets;
- Computer servers (on or off-site) that store PHI;
- Computer network (including any local and wide area networks, communications servers and bandwidth connections, and storage devices and hardware);
- Databases where patient information is created, stored, and accessed by PRO, whether on or off-site;
- Electronic media that store e-PHI such as hard drives, disks, CDs, DVDs, USB drives or other storage devices, transmission media, or portable electronic media;
- Electronic devices used for processing patient information (such as laptops and field data collection devices);
- Workstations and access points where PHI is created, accessed and used;
- Policies and procedures (written and unwritten) that involve the creation, use, or access to e-PHI; and
- Vendors, billing companies, clearinghouses and others who create, receive, maintain or transmit PHI for PRO.

### Procedure

The HIPAA Compliance Officer will utilize PRO's HIPAA Risk Analysis Tool to identify all current and potential risks and vulnerabilities to PHI at PRO and to develop a plan to manage those risks.

***Annual Risk Analysis***

PRO will, on an annual basis, undertake a risk analysis that includes the following:

1. Identifying and documenting all places where the physical (paper) PHI and e-PHI is stored, received, maintained or transmitted at PRO (*e.,* all sources of PHI at PRO whether on or off-site).
2. Identifying and documenting all current and potential risks to the confidentiality, security, integrity and availability of all PHI sources identified at PRO.
3. Assessing the likelihood of each identified risk and assigning the risk to a "risk level" and "potential impact" category.
4. Identifying and documenting any measures that PRO currently has in place to address each identified risk, including any policies, procedures, hardware/software, security devices, etc. Then, identifying any methods that are not currently in place that may eliminate or mitigate the risk.
5. Providing recommendations to PRO that might remedy identified risks and vulnerabilities and improve the security, integrity and availability of all PHI sources identified at PRO.
6. Implementing methods that might remedy identified risks and vulnerabilities and improve the security, integrity and availability of all PHI sources identified at PRO.

***Implementation Specifications***

Implementation specifications under HIPAA that are "required" must be implemented and documented that they were in fact implemented, including how the specification was implemented. Implementation specifications under HIPAA that are "addressable" will be implemented as follows:

1. If the implementation specification is reasonable and appropriate, PRO will implement it.
2. If the implementation specification is determined to be inappropriate and/or unreasonable, but the security standard cannot be met without implementation of an additional security safeguard, PRO may implement an alternative measure that achieves the addressable specification.
3. If PRO meets the standard through alternative measures, the decision not to implement the specification will be documented, including the reason for the decision, the rationale, and a description of the alternative safeguard that was implemented.

# Pro Policy 1200.2

## Policy 2: Policy on Patient Requests for Access to PHI

### Purpose

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") grants individuals the right to access their protected health information ("PHI") contained in a designated records set ("DRS"). (*See*, Policy on Designated Records Sets). PRO must afford individuals this right of access in accordance with federal and state law. To ensure that PRO complies with its obligations, this policy outlines our procedures for handling requests for patient access and establishes the procedures by which patients or authorized representatives may request access to PHI.

### Scope

This policy applies to all PRO staff members who receive requests from patients for access to PHI. Generally, all access requests will be directed to the HIPAA Compliance Officer and it shall be the responsibility of the HIPAA Compliance Officer to handle all access requests.

### Procedure

***Requests for Access from the Patient or the Patient's Personal Representative***

Patients and their authorized representatives shall be granted a right of access to inspect and obtain a copy of their PHI contained in a DRS maintained by PRO.

If a patient or their authorized representative requests access to or a copy of a patient's PHI, the requestor shall be referred to the HIPAA Compliance Officer. The HIPAA Compliance Officer shall request that the patient or authorized representative complete PRO's "Request for Access to Protected Health Information" Form.

The HIPAA Compliance Officer must verify the patient's identity, or, if the requestor is not the patient, the name and identity of the representative and whether the representative has the authority to act on the patient's behalf. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for this purpose. If it is impossible for the requestor to physically come in to make the request and verify this information, the HIPAA Compliance Officer shall ask the requestor to verify the patient's name, date of birth, SSN, address, and telephone number over the phone and ask the requestor to submit the "Request for Access to Protected Health Information Form" via email, mail or fax.

Upon receipt of the completed "Request for Access to Protected Health Information Form" and verification of the requestor's identity, the HIPAA Compliance Officer will act upon the request within 30 days, preferably sooner. Generally, PRO must respond to requests for access to PHI within 30 days of receipt of the access request.

If PRO is unable to respond to the request within these time frames, the requestor must be given a written notice no later than the initial due date for a response, explaining why PRO could not respond within the time frame, and in that case PRO may extend the response time by an additional 30 days.

***Requests for Access from the Patient's Attorney***

If PRO receives a request for a patient's PHI from the patient's attorney, the HIPAA Compliance Officer shall verify that the patient has authorized the release of PHI. Generally, the request should be accompanied by a form or letter, signed by the patient, stating that the patient authorizes the release of the requested PHI to the attorney. If there is a signed form or letter from the patient authorizing the release of the PHI requested (or some other valid authorization from the patient), then the HIPAA Compliance Officer may release the PHI to the attorney in accordance with what the authorization states.

If the request from the patient's attorney is not accompanied by a signed request form or letter from the patient (or some other valid patient authorization), the HIPAA Compliance Officer shall contact the attorney and inform the attorney that PRO will not release the information without valid authorization from the patient. PRO shall not release any PHI to the attorney until the patient authorizes the release.

***Approval of a Request for Access***

Upon approval of access, the patient or authorized representative should generally be provided the right of access in the manner requested on the Form. PRO will either provide a copy of the PHI to the requestor in the format requested or arrange for a convenient time for the patient to come into PRO to copy their PHI. If PRO uses or maintains the PHI requested electronically, PRO will provide a copy of the PHI in an electronic format if the patient or authorized representative requests an electronic copy. PRO will also transmit a copy of the PHI directly to an entity or person designated by the patient or authorized representative, provided that the written direction is signed and clearly identifies the designated party.

PRO will establish a reasonable charge for copying PHI for the patient or authorized representative in accordance with federal and state laws. The fee for providing an electronic copy of PHI shall not be greater tha PRO's labor costs in responding to the request for the copy. The HIPAA Compliance Officer shall consult with legal counsel regarding applicable laws regarding fee limitations.

The requestor will not be given access to the actual files or systems that contain the DRS. Rather, copies of the records shall be provided for the patient or requestor to view in a confidential area under the direct supervision of a designated Company staff member. UNDER NO CIRCUMSTANCES SHOULD ORIGINALS OF PHI LEAVE THE PREMISES.

Whenever a patient or requestor accesses a DRS, a note should be maintained in a log book indicating the time and date of the request, the date access was provided, what specific records were provided for review, and what copies were left with the patient or requestor.

***Denial of a Request for Access***

If the request for access is denied, the HIPAA Compliance Officer shall send the requestor a "Denial of Request for Access to Protected Health Information Form," outlining the reason for the denial and explaining the individual's rights regarding the denial. Patient access may be denied for the reasons listed below:

1. If the information the patient requested was compiled in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding;

2. If the information the patient requested was obtained from someone other than a healthcare provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information;
3. If a licensed healthcare professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
4. If the PHI makes reference to another person (other than a healthcare provider) and a licensed health professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to that person; or
5. If the request for access is made by a requestor as a personal representative of the individual and a licensed health professional has determined, in the exercise of professional judgment, that access is reasonably likely to cause harm to the individual or another person.

If the denial of the request for access to PHI is for reasons c., d., or e. above, then the patient may request a review of the denial of access by sending a written request to the HIPAA Compliance Officer.

1. PRO will designate a licensed health professional, who was not directly involved in the denial, to review the decision to deny the patient access. PRO will promptly refer the request to this designated review official. The review official will determine within a reasonable period of time whether the denial is appropriate. PRO will provide the patient with written notice of the determination of the designated reviewing official.
2. The patient may also file a complaint in accordance with PRO's "Procedure for Filing Complaints About Privacy Practices" if the patient is not satisfied with PRO's determination.

# Pro Policy 1200.3

## Policy 3: Policy on Patient Requests for Amendment of PHI

### Purpose

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") grants individuals the right to request that PRO amend their protected health information ("PHI") contained in a Designated Record Set ("DRS"). (*See*, Policy on Designated Record Sets). PRO has an obligation to afford individuals the right to request an amendment to their PHI in accordance with federal and state law. To ensure that PRO complies with its obligations, this policy outlines procedures for handling patient requests for amendment of their PHI and establishes the procedures by which patients or authorized representatives may make a request for an amendment to PHI.

### Scope

This policy applies to all PRO staff members who handle requests from patients for amendment to PHI. Generally, all requests will be directed to the HIPAA Compliance Officer and it shall be the responsibility of the HIPAA Compliance Officer to handle all requests for amendment of PHI.

### Procedure

***Requests for Amendment of PHI***

1. Patients or their authorized representatives shall be granted the right to request an amendment to a patient's PHI contained in the DRS.
2. If a patient or authorized representative requests an amendment to PHI, the requestor shall be referred to the HIPAA Compliance Officer. The HIPAA Compliance Officer shall request that the patient or authorized representative complete PRO's "Patient Request for Amendment of Protected Health Information" Form.
3. The HIPAA Compliance Officer must verify the patient's identity, or, if the requestor is not the patient, the name and identity of the representative and whether the representative has the authority to act on the patient's behalf. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for this purpose. If it is impossible for the requestor to physically come in to make the request and verify this information, the HIPAA Compliance Officer shall ask the requestor to verify the patient's name, date of birth, SSN, address, and telephone number over the phone and ask the requestor to submit the "Request for Amendment of Protected Health Information Form" via email, mail or fax.
4. PRO must act upon a request for amendment of PHI within 60 days of the request. If PRO is unable to act upon the request within 60 days, it must provide the requestor with a written statement of the reasons for the delay, and in that case may extend the time period in which to comply by an additional 30 days.

***Granting the Request for Amendment of PHI***

1. If the HIPAA Compliance Officer grants the request for amendment, then the requestor will receive a letter (*See*, "Acceptance of Patient Request for Amendment" Form), indicating that the appropriate amendment to the PHI or record that was the subject of the request has been made.

2. The letter will contain a form for the patient to complete, sign, and return to PRO. On the form, the patient must identify individuals who may need the amended PHI and sign the statement giving PRO permission to provide them with the updated PHI.
3. PRO must provide the amended information to individuals identified by the patient as well as persons or business associates that have such information and who may have relied on or could be reasonably expected to rely on the amended PHI.

***Denying the Request for Amendment of PHI***

PRO may deny a request to amend PHI for the following reasons:

1. If PRO did not create the PHI at issue;
    a. The information is not part of the DRS;
    b. The PHI is accurate and complete;
    c. The information would not be available for inspection as provided by law; or
    d. The information was received from someone else under a promise of confidentiality.
2. PRO must provide a written denial (*See*, "Denial of Patient Request for Amendment" Form), and the denial must be written in plain language and contain the following information:
    a. The reason for the denial;
    b. The individual's right to submit a statement disagreeing with the denial and how the individual may file such a statement;
    c. A statement that, if the individual does not submit a statement of disagreement, the individual may request that PRO provide the request for amendment and the denial with any future disclosures of the PHI; and
    d. A statement that the individual may file a complaint with PRO or with the Office for Civil Rights of the Department of Health and Human Services.
3. PRO shall provide a copy of our "Procedure for Filing Complaints About Privacy Practices" if the requestor indicates that he or she wants to file a complaint against PRO.
4. If the individual submits a "statement of disagreement," PRO may prepare a written rebuttal statement to the patient's statement of disagreement. The statement of disagreement will be appended to the PHI, or at PRO's option, a summary of the disagreement will be appended, along with the rebuttal statement of PRO.

***Administrative Obligations***

1. If PRO receives a notice from another covered entity, such as a hospital, that the other covered entity has amended its own PHI in relation to a particular patient, PRO must amend its own PHI that may be affected by the amendments. The HIPAA Compliance Officer shall be responsible for performing this task.
2. PRO will add the "Patient Request for Amendment of Protected Health Information Form," the denial or granting of the request, as well as any statement of disagreement by the patient and any rebuttal statement by PRO to the DRS. The HIPAA Compliance Officer shall be responsible for performing this task.

## Pro Policy 1200.4

Policy 4: Policy on Patient Requests for Restriction of PHI

## Purpose

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") grant individuals the right to request that PRO restrict its use of PHI contained in a Designated Record Set ("DRS"). (*See*, Policy on Designated Record Sets). PRO has an obligation to abide by a requested restriction in accordance with federal and state law. To ensure that PRO complies with its obligations under HIPAA and the HITECH Act, this policy outlines procedures for handling requests for restrictions on the use of PHI and establishes the procedures by which patients or their authorized representatives may request a restriction on the use of PHI.

## Scope

This policy applies to all PRO staff members who handle requests from patients for a restriction on the use of their PHI. Generally, all requests will be directed to the HIPAA Compliance Officer and it shall be the responsibility of the HIPAA Compliance Officer to handle all requests for restrictions on the use of PHI.

## Procedure

***Requests for Restriction***

1. PRO will permit patients to request restrictions on the use and disclosure of their PHI: (i) to carry out treatment, payment or health care operations and/or (ii) to people involved in their care or for notification purposes.
2. All requests for restriction on the use and disclosure of PHI shall be referred to the HIPAA Compliance Officer who shall request that the patient or authorized representative complete and submit PRO's "Patient Request for Restriction of Protected Health Information" Form. All requests will be reviewed and denied or approved by the HIPAA Compliance Officer in accordance with this policy. The HIPAA Compliance Officer shall utilize the "Review of Patient Request for Restriction of Protected Health Information" Form when reviewing restriction requests.
3. The HIPAA Compliance Officer must verify the patient's identity, or, if the requestor is not the patient, the name and identify of the representative and whether the representative has the authority to act on the patient's behalf. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for this purpose. If it is impossible for the requestor to physically come in to make the request and verify this information, the HIPAA Compliance Officer shall ask the requestor to verify the patient's name, date of birth, SSN, address, and telephone number over the phone and ask the requestor to submit the "Patient Request for Restriction of Protected Health Information" Form via email, mail or fax.
4. Under most circumstances, PRO is not legally required to agree to any request to restrict the use and disclosure of PHI, and given the emergent nature of our operation, PRO generally will not agree to a restriction unless required by law to do so. However, PRO is required to abide by any restrictions that it agrees to.

***Granting a Request for Restriction***

1. PRO will and must comply with a requested restriction if: (i) the request concerns the disclosure of PHI to a health plan for purposes of carrying out payment or healthcare operations; and (ii) the request pertains to a service for which PRO has been paid out-of-pocket in full. In other words, PRO must grant patients the right to pay for a service out-of-pocket and abide by a request not to submit a claim to the insurer for that service.
2. If PRO receives a request from a patient or authorized representative asking PRO to refrain from submitting PHI to a health plan and the HIPAA Compliance Officer determines that PRO has either been paid in full, or that PRO has received reasonable assurances that it will be paid in full for that service, then PRO will grant the request for restriction and not submit a claim to insurance for that service. Patients must make a new request for all subsequent services.
3. If PRO agrees to a requested restriction, the HIPAA Compliance Officer shall inform the patient of that fact in writing, by sending an "Acceptance of Request for Restriction of Protected Health Information" letter to the patient. The HIPAA Compliance Officer shall also note on the "Review of Patient Request for Restriction of Protected Health Information" Form that the request was accepted and document all pertinent information regarding the request and acceptance (date, payment received, etc.).
4. PRO may not use or disclose PHI in violation of the agreed upon restriction. Notwithstanding, if the individual who requested the restriction is in need of an emergency service, and the restricted PHI is needed to provide the emergency service, then PRO may use the restricted PHI or may disclose such PHI to another healthcare provider to provide treatment to the individual.
5. The HIPAA Compliance Officer shall also inform all other necessary parties at PRO and its business associates, such as its billing company, about the accepted restriction and take all appropriate steps to ensure that those parties abide by the restriction.
6. The HIPAA Compliance Officer shall add the "Patient Request for Restriction of Protected Health Information" Form, the Acceptance letter and documentation regarding the acceptance of the request to the DRS.

***Denying the Request for Restriction***

1. Unless PRO is required by law to agree to a request for restriction of PHI, the HIPAA Compliance Officer shall deny the request in writing, by dispatching a "Denial of Patient Request for Restriction of PHI" letter to the patient.
2. The HIPAA Compliance Officer shall also note on the "Patient Request for Restriction of Protected Health Information" Form that the request was denied, and document all pertinent information regarding the request and denial (date, reason for denial, etc.).

***Termination of Restrictions***

1. A restriction may be terminated if the individual agrees to or requests the termination.
2. Oral agreements to terminate restrictions must be documented.
3. Most restrictions may also be terminated by PRO as long as PRO notifies the patient that PHI created or received after the restriction is removed is no longer restricted. PHI that was restricted prior to the notice voiding the restriction must continue to be treated as restricted PHI.
4. PRO should not terminate a restriction regarding PHI that pertains to a service for which PRO has been paid in full and where a patient has requested that such PHI not be disclosed to the patient's health plan. Such restriction will only apply with respect to that service and not to

subsequent services. The patient must make another request, and pay out-of-pocket for each service.

# Pro Policy 1200.5

## Policy 5: Policy on Patient Requests for Accounting of Disclosures of PHI

### Purpose

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") grants individuals the right to an accounting of disclosures of their protected health information ("PHI") from paper and electronic records. PRO has an obligation to render an accounting to individuals in accordance with federal and state law. To ensure that PRO complies with its obligations, this policy outlines our procedures for handling requests for an accounting and establishes the procedures by which patients or their authorized representatives may request an accounting of disclosures of PHI from PRO.

### Scope

This policy applies to all PRO staff members who receive requests from patients for an accounting of disclosures of PHI. Generally, all requests will be directed to the HIPAA Compliance Officer and it shall be the responsibility of the HIPAA Compliance Officer to handle all accounting requests.

### Procedure

***Requests for an Accounting***

Patients and their authorized representatives shall have a right to request an accounting of certain disclosures of PHI made by PRO.

1. If a patient or their authorized representative requests an accounting of disclosures of PHI, the requestor shall be referred to the HIPAA Compliance Officer. The HIPAA Compliance Officer shall request that the patient or authorized representative complete PRO's "Patient Request for Accounting of Disclosures Protected Health Information" Form.
2. The HIPAA Compliance Officer must verify the patient's identity, or, if the requestor is not the patient, the name and identity of the representative and whether the representative has the authority to act on the patient's behalf. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for this purpose. If it is impossible for the requestor to physically come in to make the request and verify this information, the HIPAA Compliance Officer shall ask the requestor to verify the patient's name, date of birth, SSN, address, and telephone number over the phone and ask the requestor to submit the "Patient Request for Accounting of Disclosures of Protected Health Information" Form via email, mail or fax.
3. Upon receipt of the completed "Patient Request for Accounting of Disclosures of Protected Health Information" Form and verification of the requestor's identity, the HIPAA Compliance Officer will respond to a request for an accounting of disclosures within 60 calendar days of receipt of a request, preferably sooner.
4. If PRO is unable to provide the accounting within 60 calendar days, PRO may extend the time for responding to the request by no more than 30 calendar days, provided that within the 60 day period PRO provides a written statement to the individual explaining the reasons for delay and the date by which the accounting will be provided. Only one 30-day extension may be exercised per accounting request.

***Fulfilling an Accounting Request***

1. PRO will provide the patient or their authorized representative with a written or electronic accounting of disclosures of their PHI made by PRO or its business associates on PRO's behalf, as required by HIPAA. PRO will render an accounting of all disclosures of PHI during the period requested by the patient or other requestor. If the requestor does not specify a time period for the accounting, PRO will render an accounting of disclosures of PHI made during the past six (6) years. The following disclosures are excluded from the HIPAA accounting requirement:
    a. Disclosures to carry out treatment, payment or health care operations;
    b. Disclosures made to the patient or to the patient's authorized representative;
    c. Disclosures incident to a use or disclosure otherwise permitted or required by HIPAA;
    d. Disclosures pursuant to the patient's authorization;
    e. Disclosures for a facility directory or to persons involved in the patient's care;
    f. Disclosures for national security or intelligence purposes;
    g. Disclosures to correctional institutions or law enforcement officials to provide them with information about a person in their custody; and
    h. Disclosure made as part of a limited data set.

    PRO will not render an accounting for disclosures that are exempt from the HIPAA accounting requirement.

2. All accountings shall include the following information regarding each disclosure of PHI addressed in the accounting:
    a. The date of the disclosure;
    b. The name of the entity or person who received the PHI and, if known, the address of such entity or person;
    c. A brief description of the PHI disclosed; and
    d. A brief statement of the purpose of the disclosure that reasonably informs the patient of the basis for the disclosure.

***Tracking Disclosures of PHI***

5. In order to fulfill its obligations to render an accounting of disclosures of PHI under HIPAA, PRO shall track all necessary disclosures of PHI. The HIPAA Compliance Officer is responsible to ensure PRO is tracking disclosures when required by HIPAA to do so.

6. Generally PRO shall track all disclosures for or pursuant to:
    a. Research purposes, unless authorized by the patient;
    b. Subpoenas, court orders or discovery requests;
    c. Abuse and neglect reporting;
    d. Communicable disease reporting; and
    e. Other reports to a Department of Health.

    The HIPAA Compliance Officer may utilize the "Accounting Log for Disclosures of PHI" Form for this purpose and track all information required on the Form.

***Administrative Requirements***

PRO shall retain the following documentation, in either written or electronic form, for 6 years:

7. Written requests by an individual for an accounting of disclosures;

8. Accountings of disclosures that have been provided to an individual, including the titles of the persons and offices responsible for receiving and processing the request for accounting; and
9. Copies of any notices to the individual explaining that PRO requires an extension of time to prepare the requested accounting.

# Pro Policy 1200.6

## Policy 6: Policy on Patient Requests for Confidential Communications

### Purpose

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") grants individuals the right to request that PRO send PHI to an alternate location (*e.g.,* somewhere other than a home address), or through alternate means (*e.g.,* by email rather than regular mail). This is called the right to "confidential communications." PRO has an obligation to grant patients this right and it must abide by a request for confidential communications of PHI in accordance with federal and state law. To ensure that PRO complies with its obligations, this policy outlines procedures for handling requests for confidential communications of PHI and establishes the procedures by which patients or their authorized representatives may request confidential communications.

### Scope

This policy applies to all PRO staff members who handle requests from patients for confidential communications of their PHI. Generally, all requests will be directed to the HIPAA Compliance Officer and it shall be the responsibility of the HIPAA Compliance Officer to handle all requests for confidential communications.

### Procedure

***Requests for Confidential Communications***

1. PRO will permit patients to request that PRO send PHI to individuals at an alternate location (*g.,* somewhere other than a home address), or in a specific manner (*e.g.,* by email rather than regular mail).
2. All requests for confidential communications PHI shall be referred to the HIPAA Compliance Officer who shall request that the patient or authorized representative complete and submit PRO's "Patient Request for Confidential Communications of Protected Health Information" Form. All requests will be reviewed and denied or approved by the HIPAA Compliance Officer in accordance with this policy. The HIPAA Compliance Officer shall utilize the "Review of Patient Request for Confidential Communications of Protected Health Information" Form when reviewing requests for confidential communications of PHI.
3. The HIPAA Compliance Officer must verify the patient's identity, or, if the requestor is not the patient, the name and identify of the representative and whether the representative has the authority to act on the patient's behalf. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for this purpose. If it is impossible for the requestor to physically come in to make the request and verify this information, the HIPAA Compliance Officer shall ask the requestor to verify the patient's name, date of birth, SSN, address, and telephone number over the phone and ask the requestor to submit the "Patient Request for Confidential Communications of Protected Health Information" Form via email, mail or fax.
4. PRO is required to and will agree to any "reasonable requests" for confidential communications.

***Granting a Request for Confidential Communications***

1. PRO will and must comply with a confidential communications request if the request is "reasonable." The HIPAA Compliance Officer shall take into account logistical reasons and other factors, such as the cost of making the alternate confidential communications, when determining whether the request is reasonable.
2. If PRO receives a request from a patient or authorized representative asking PRO to communicate PHI in an alternate manner and PRO determines that the request is reasonable, it will agree to the request and the HIPAA Compliance Officer shall inform the patient of that fact, in writing, by sending an "Acceptance of Request for Confidential Communications of Protected Health Information" letter to the patient. The HIPAA Compliance Officer shall also note on the "Review of Patient Request for Confidential Communications of Protected Health Information" Form that the request was accepted and document all pertinent information regarding the request and acceptance.

***Denying the Request for Confidential Communications***

1. If the HIPAA Compliance Officer determines, after taking into account logistical reasons and other factors, that the request is not reasonable, the HIPAA Compliance Officer shall deny the request, in writing, by dispatching a "Denial of Patient Request for Confidential Communications of PHI" letter to the patient.
2. The HIPAA Compliance Officer shall also note on the "Review of Patient Request for Confidential Communications of Protected Health Information" Form that the request was denied, and document all pertinent information regarding the request and denial.

# Pro Policy 1200.7

## Policy 7: HIPAA Compliance Officer Action Plan for Patient Requests Relating to PHI

Step 1: Whenever a request is made regarding a patient's PHI, the HIPAA Compliance Officer must first verify that the requestor is the patient. Or, if the requestor is not the patient, the HIPAA Compliance Officer must verify the name and identity of the requestor and verify whether the requestor has the authority to act on the patient's behalf as a personal representative. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for making this verification. If it is impossible for the requestor to physically come in to make the request and verify this information, the HIPAA Compliance Officer shall ask the requestor to verify the patient's name, date of birth, SSN, address, and telephone number over the phone and ask the requestor to submit the appropriate request form via email, mail or fax.

Step 2: The HIPAA Compliance Officer will ask the requestor what type request is being made, provide the requestor with the appropriate request form, and handle the request in accordance with the appropriate policy. The general process for handling patient requests regarding PHI is outlined in this Action Plan.

### Request for Access to PHI – Request Form

The HIPAA Compliance Officer shall request that the patient or authorized representative complete PRO's "Request for Access to Protected Health Information" Form.

### Request for Access to PHI – General Procedure

Upon receipt of the completed "Request for Access to Protected Health Information" Form, the HIPAA Compliance Officer will act upon the access request within 30 days, preferably sooner. The HIPAA Compliance Officer will proceed to handle the request in accordance with PRO's "Policy on Patient Requests for Access to Protected Health Information." Most access requests must be granted within 30 days.

### Request for Amendment of PHI – Request Form

The HIPAA Compliance Officer shall request that the patient or authorized representative complete PRO's "Patient Request for Amendment of Protected Health Information" Form.

### Request for Amendment of PHI – General Procedure

Upon receipt of the completed "Patient Request for Amendment of Protected Health Information" Form, the HIPAA Compliance Officer must either grant or deny the patient's amendment request within 60 days in accordance with PRO's "Policy on Patient Requests for Amendment of Protected Health Information." Many requests for amendment will be denied if PRO determines that the current record that the requestor is asking PRO to amend is true and correct.

Request for Restriction of PHI – Request Form

The HIPAA Compliance Officer shall request that the patient or authorized representative complete and submit PRO's "Patient Request for Restriction of Protected Health Information" Form.

Request for Restriction of PHI – General Procedure

Upon receipt of the completed "Patient Request for Restriction of Protected Health Information" Form, the request will be reviewed and denied or approved by the HIPAA Compliance Officer in accordance with PRO's "Policy on Patient Requests for Restriction of Protected Health Information," as soon as possible. The HIPAA Compliance Officer shall utilize PRO's "Review of Patient Request for Restriction of Protected Health Information" Form when reviewing restriction requests. Under most circumstances, PRO is not legally required to agree to any request to restrict the use and disclosure of PHI and PRO generally will not agree to a restriction unless required by law to do so. PRO is required to agree to a restriction if a patient pays PRO in full for a service and requests that PRO not to submit a claim to the patient's insurer for that service.

Request for Accounting of Disclosures of PHI – Request Form

The HIPAA Compliance Officer shall request that the patient or authorized representative complete PRO's "Patient Request for Accounting of Disclosures Protected Health Information" Form.

Request for Accounting of Disclosures of PHI – General Procedure

Upon receipt of the completed "Patient Request for Accounting of Disclosures of Protected Health Information" Form, the HIPAA Compliance Officer will respond to a request for an accounting of disclosures within 60 calendar days of receipt of a request in accordance with PRO's "Policy on Requests for Accounting of Disclosures of Protected Health Information." PRO will render an accounting of certain disclosures of PHI during the period requested, or, if the requestor does not specify a time period for the accounting, PRO will render an accounting for certain disclosures of PHI made during the past six (6) years. However, most disclosures are excluded from the HIPAA accounting requirement, including disclosures related to treatment, payment or health care operations. PRO will not render an accounting for disclosures that are exempt from the HIPAA accounting requirement.

## Requests for Confidential Communications – Request Form

Individuals can request that PRO send PHI to an alternate location (*e.g.,* somewhere other than a home address), or through alternate means (*e.g.,* by email rather than regular mail). This is called the right to "confidential communications." Upon receipt of a request for confidential communication of PHI, the HIPAA Compliance Officer shall request that the patient or authorized representative complete and submit PRO's "Patient Request for Confidential Communications of Protected Health Information" Form.

## Requests for Confidential Communications – General Procedure

All requests for confidential communications of PHI will be reviewed and denied or approved by the HIPAA Compliance Officer in accordance with PRO's "Policy on Patient Requests for Confidential Communications of Protected Health Information." The HIPAA Compliance Officer shall utilize the "Review of Patient Request for Confidential Communications of Protected Health Information" Form when reviewing these requests. PRO will and must comply with a requested confidential communications request if the request is "reasonable." If PRO agrees to the request, the HIPAA Compliance Officer shall inform the patient of that fact in writing, by sending a version of PRO's "Acceptance of Request for Confidential Communications of Protected Health Information" letter to the patient.

# Pro Policy 1200.8

## Policy 8: Policy on HIPAA Training

### Purpose

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires that all members of PRO's workforce be trained on our policies and procedures regarding privacy and security. This policy is meant to ensure that all of PRO staff – including all employees, volunteers, students and trainees (collectively referred to as "staff members") – who have access to protected health information ("PHI") understand and are trained regarding PRO's HIPAA policies and procedures.

### Scope

This policy applies to all PRO staff members. This includes those who have access to PHI in any form

### Procedure

1. All current staff members must be trained on PRO's HIPAA policies and procedures in accordance with HIPAA.
2. All new staff members will be required to undergo privacy training within a reasonable time upon association with PRO.
3. All staff members who have undergone initial HIPAA training will be required to undergo HIPAA training within a reasonable time after there is a material change to PRO's HIPAA policies and procedures.
4. The HIPAA training will be coordinated and tracked on the "HIPAA Training Log" Form by the HIPAA Compliance Officer or his or her designee. Training documentation will be maintained for six (6) years.
5. All staff members will receive copies of PRO's HIPAA policies and procedures.
6. All staff members must personally complete the HIPAA training and verify completion and agree to adhere to PRO's HIPAA policies and procedures.
7. Training will be conducted through the following method: PWW HIPAA TV.
8. All staff members shall sign the "HIPAA Training Log" after completing HIPAA training.

# Pro Policy 1200.9

## Policy 9: Policy on Updating HIPAA Policies, Procedures & Training

### Purpose

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires PRO to ensure that its HIPAA policies, procedures and training materials are up to date and effective in safeguarding the confidentiality, integrity and availability of protected health information ("PHI"). This policy outlines our commitment to adjust and update our policies and procedures accordingly, based on periodic reviews and evaluations of our existing practices and in light of new and changing risks to PHI. PRO will also evaluate and consider new technologies and methodologies for securing PHI, as specified by guidance from the Secretary of Health and Human Services ("HHS").

### Scope

This policy applies to all PRO staff members who are responsible for evaluating and updating current HIPAA policies and procedures and providing the updates to staff members. The HIPAA Compliance Officer will have the overall responsibility for monitoring all new developments in patient privacy and security of PHI and will recommend updates to our HIPAA Compliance Program, as necessary. The HIPAA Compliance Officer should perform these duties in consultation with PRO management and solicit the input of appropriate PRO staff members, when appropriate.

### Procedure

***Maintaining Knowledge***

1. The HIPAA Compliance Officer will strive to keep current with all changes in the law and regulations that address the privacy and security of PHI.
2. The HIPAA Compliance Officer will review journals and newsletters on the subject of HIPAA, and will sign up for appropriate list-serves to obtain current information.
3. The HIPAA Compliance Officer will monitor HIPAA websites, such as the site for the Office of Civil Rights, for new information on HIPAA compliance.
4. The HIPAA Compliance Officer will participate in seminars and conferences on HIPAA as needed and as the budget allows.
5. The HIPAA Compliance Officer will consult with legal counsel as necessary to learn of new legal developments that could affect PRO with respect to HIPAA issues.

***Evaluation of HIPAA Policies and Procedures***

1. On at least an annual basis, the HIPAA Compliance Officer will convene a committee of managers and/or appropriate staff members to identify and review all existing HIPAA policies and procedures for compliance with current HIPAA laws and regulations.
2. Any member of the review committee or any other staff member may suggest changes to our HIPAA Policies or Procedures by submitting the suggestion to the HIPAA Compliance Officer for consideration.
3. The annual policy and procedure review will identify all changes that need to be made to our policies, based on the experience of staff and management, technological developments and changes in the regulatory environment during the prior year.

4. Any critical changes in the law or regulations that require a change in our privacy practices will be addressed immediately and incorporated into our privacy compliance program.
5. All complaints and concerns regarding the safeguarding of patient information will be evaluated by the HIPAA Compliance Officer to determine if policy or procedure changes need to be implemented.
6. Unwritten procedures and practices will also be reviewed to ensure compliance with HIPAA regulations.

***Evaluating and Updating HIPAA Training Programs***

1. The HIPAA Compliance Officer annually reviews all HIPAA-related training materials and will update those materials and keep them current with recent changes in privacy practices as necessary.
2. Additional in-service training will be scheduled as necessary to ensure that all current staff members are kept up to date on our current HIPAA policies and procedures.

# Pro Policy 1200.10

## Policy 10: Policy on Contracting With Business Associates

### Purpose

PRO is responsible for ensuring the privacy and security of all protected health information ("PHI") that we create, receive, maintain or transmit under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HIPAA requires that PRO ensure that those persons and entities that perform services on our behalf using PHI agree to protect that PHI as we would by requiring those parties to sign a "business associate agreement" ("BAA") with PRO. This policy describes our approach to entering into business associate agreements with persons and organizations that perform services on our behalf involving the use of PHI.

### Scope

This policy applies to all PRO staff members who are responsible for entering into agreements with outside vendors or persons who might have access to PHI. Generally, the HIPAA Compliance Officer of PRO is responsible to initiate a business associate agreement with any person or entity that performs a service on behalf of PRO that involves the use or disclosure of PHI.

### Procedure

1. The HIPAA Compliance Officer is responsible for identifying persons and organizations that perform services on our behalf and who in any manner create, receive, maintain or transmit PHI about our patients. All such persons or entities are called "business associates" ("BAs") of PRO. For example, our business associates include, but are not limited to, our outside billing company, our outside consultants, and our outside attorney. Workforce members are not business associates, nor are organizations that share a direct treatment relationship with patients to whom PRO provides services. When in doubt, the HIPAA Compliance Officer should consult qualified legal counsel when determining whether an entity meets the legal definition of a BA.
2. All identified BAs of PRO must enter into a BAA if they wish to do business with us. Even if we do not have a written services contract with a party, HIPAA requires that we have a written business associate agreement with all BAs. No disclosures of PHI will be made by PRO to a BA until the BAA has been signed.
3. Whenever possible, PRO will use its standard business associate agreement. If the BA insists on using its own business associate agreement, the HIPAA Compliance Officer must ensure that the agreement proposed by the BA conforms to HIPAA's requirements.
4. Whenever PRO modifies its existing business associate agreement, the HIPAA Compliance Officer shall ensure that we enter into a new business associate agreement with our current BAs.
5. Whenever possible, all contracts and service agreements between PRO and any BA should include the relevant business associate language directly in the contract or service agreement. Otherwise, a stand-alone business associate agreement is required. If there is a business associate agreement separate from the main contract or service agreement, then the main agreement must specifically refer to the business associate agreement.
6. The HIPAA Compliance Officer will maintain a current list of business associates.

7. At times, PRO may be asked to enter into business associate agreements. The HIPAA Compliance Officer shall evaluate the appropriateness of the business associate agreement under the circumstances and enter into the agreement only when required by law and if the agreement meets the legal requirements under HIPAA.
8. The HIPAA Compliance Officer is responsible for maintaining BA agreements on file for periodic review and inspection.
9. With respect to a person or entity that is not a BA, but which may potentially come into contact with PHI, such as janitorial services or information technology service providers, the HIPAA Compliance Officer should seek to have a “Confidentiality Agreement” in place with the entity.

# Pro Policy 1200.11

## Policy 11: Policy on Workforce Sanctions for Violations of HIPAA Policies and Procedures

### Purpose

PRO is responsible under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to administer appropriate sanctions to its workforce members who violate the HIPAA policies and procedures of the organization. This policy outlines our approach to violations of our HIPAA policies and procedures and emphasizes the fact that PRO takes any breach of our policies and procedures very seriously.

### Scope

This policy applies to all PRO staff members, including those staff members who may learn of patient information indirectly, and even if use of this information is not part of the staff member's responsibilities with PRO.

NOTE: Any sanctions under this policy or any other policy will not apply to staff members who 1) file a complaint with the federal government about potential HIPAA violations, 2) testify, assist, or participate in an investigation or compliance review proceeding or official government proceeding investigating HIPAA issues, and 3) oppose any actions by PRO that are unlawful under HIPAA, when that opposition is made with the good faith belief that PRO was violating HIPAA (as long as any opposition or filing of a complaint did not result in improper disclosure of PHI).

### Procedure

1. PRO will implement sanctions that are to be used when any staff member fails to comply with or violates our HIPAA policies and procedures.
2. Sanctions will be administered in a progressive manner, wherever possible. PRO will administer sanctions to the degree necessary to correct improper behavior and to ensure the protection of patient privacy. The nature of the PHI involved in the incident will be considered.

   (EXAMPLE: A first time violation where an employee revealed PHI to another staff member without any need to know may receive a verbal counseling or written warning, but if a first violation resulted in revealing PHI to someone who was not a staff member or business associate, a suspension may be warranted.)

3. Progressive sanctions may include the following:
   a. Remedial HIPAA training and education
   b. Informal verbal counseling
   c. Formal verbal counseling with written documentation of the counseling
   d. Written warning
   e. Suspension
   f. Termination or expulsion from PRO
4. Staff members have an affirmative duty to report to management or the HIPAA Compliance Officer any suspected violation of our HIPAA policies and procedures.

5. Staff members shall be educated about this policy and the serious nature of violating our HIPAA policies. Staff members will be made aware of the potential sanctions that may occur, and will be made aware of any changes to this sanction policy.
6. A record of individual staff member sanctions will be kept in the respective staff member's file. Adherence to our HIPAA policies may also be considered as part of the staff member's performance evaluation.
7. In the event of a suspected or reported violation of our HIPAA policies, the HIPAA Compliance Officer will initiate an objective and comprehensive investigation that will include:
    a. Interviews of potential witnesses
    b. Interviews of the alleged violator
    c. Preparation of an investigative report
    d. Presentation of the report to management with recommendations for sanctions (if any) or changes in our policies or practices
8. At all times, whenever there is a suspected violation of our HIPAA policies or other breach of privacy, the HIPAA Compliance Officer will recommend immediate action to be taken to mitigate the violation and its impact on PRO and any other parties.

# Pro Policy 1200.12

## Policy 12: Policy on Minimum Necessary Requirement & Role-Based Access to PHI

### Purpose

Generally, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires that PRO only use or disclose the minimum amount of protected health information ("PHI")that is needed to accomplish the intended purpose for which the use or disclosure is made. This policy outlines PRO's commitment to adhere to HIPAA's "minimum necessary requirement." In order to effectively meet our obligations, this policy outlines the appropriate levels of access to PHI that specific staff members of PRO should have – "Role Based Access." This policy does not in any way limit the amount of PHI that may be exchanged between PRO staff members or between PRO staff members and other individuals during the course of treating patients.

### Scope

This policy applies to all PRO staff members who have any degree of access to PHI at PRO.

### Procedure

PRO retains strict requirements on the security, access, disclosure and use of PHI. Access, disclosure and use of PHI will be based on the role of the individual staff member in the organization, and only to the extent that the person needs to access and use the PHI to complete necessary responsibilities for PRO. When PHI is accessed, disclosed and used, the individuals involved will make every effort, except in patient care situations, to only access, use, and disclose the minimum necessary amount of information needed to accomplish the intended purpose.

***Role Based Access***

Access to PHI will be limited to those who need access to carry out their duties. The following table describes the specific categories or types of PHI to which identified persons need access, and any conditions that would apply to such access.

| Job Title | Description of PHI to Be Accessed | Conditions of Access to PHI |
|---|---|---|
| EMT | Intake information from dispatch, patient care reports, QA and QI reports | May access only as part of completion of a patient event and post-event activities and only while actually on duty |
| Paramedic | Intake information from dispatch, patient care reports, QA and QI reports | May access only as part of completion of a patient event and post-event activities and only while actually on duty |
| Billing Clerk | Intake information from dispatch, patient care reports, billing claim information, remittance advice, other patient information from facilities necessary for billing | May access only as part of duties to complete patient billing and follow up and only while actually on duty |

| | | |
|---|---|---|
| Field Supervisor | Intake information from dispatch, patient care reports, QA and QI reports | May access only as part of completion of a patient event and post-event activities, as well as for quality assurance checks and corrective counseling of staff |
| Dispatcher | Intake information, preplanned CAD information on patient address | May access only as part of completion of an incident, from receipt of information necessary to dispatch a call, to the closing out of the incident and only while on duty |
| Training Coordinator | Intake information from dispatch, patient care reports, QA and QI reports | May access only as a part of training and quality assurance activities. All individually identifiable patient information should be redacted prior to use in training and quality assurance activities |
| Managers | Intake information from dispatch, patient care reports, QA and QI reports, billing claim forms, remittance advice, other patient information necessary for oversight | May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel and compliance with the law |

Access to a patient's entire file will not be allowed except when necessary for a legitimate treatment, payment, or healthcare operations-related reason.

Disclosures to and Authorizations from the Patient

PRO may freely disclose PHI to patients who are the subject of the information and we may freely use and disclose PHI to the extent authorized by a patient. PRO is required to limit disclosure to the minimum amount of information necessary when releasing it pursuant to a patient request or formal Authorization.

***PRO Requests for PHI from Other Parties***

If PRO needs to request PHI from another party on a routine or recurring basis, we must limit our requests to only the minimum amount of information needed for the intended purpose, as described in the table below. For requests not addressed in the table below, PRO must make this determination individually for each request, and this determination should be made by the HIPAA Compliance Officer. For example, if the request is non-recurring or non-routine, like making a request for documents pursuant to an audit request, we must make sure our request covers only the minimum necessary amount of information needed to accomplish the purpose of the request.

| Holder of PHI | Purpose of Request | Information Reasonably Necessary |
|---|---|---|
| Skilled Nursing Facilities | To have adequate patient records to treat the patient, determine medical necessity for service, and to properly bill for services provided | Patient face sheets, discharge summaries, Physician Certification Statements and Statements of |

| | | |
|---|---|---|
| | | Medical Necessity, Mobility Assessments |
| Hospitals | To have adequate patient records to treat the patient, determine medical necessity for service, and to properly bill for services provided | Patient face sheets, discharge summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments |
| Mutual Aid Ambulance or Paramedic Services | To have adequate patient records to treat the patient, conduct joint billing operations for patients mutually treated/transported by the Company | Patient care reports |

***PHI Requests to PRO from Other Parties***

PRO will make reasonable efforts to release only the minimum amount of PHI that is necessary to accomplish the actual purpose of a request from a third party.

***Incidental Disclosures***

PRO understands that there will be times when there are incidental disclosures about PHI in the context of caring for a patient. HIPAA was not intended to impede common healthcare practices that are essential in providing healthcare to the individual. Incidental disclosures are inevitable, but these will typically occur in radio or face-to-face conversations between healthcare providers, or when PHI is able to be viewed by others, despite reasonable efforts to protect the PHI from view.

But all personnel must be sensitive to avoiding incidental disclosures to other healthcare providers and others who do not have a need to know the information. PRO staff should be attentive to who is within earshot when making verbal statements about a patient's health information, and follow some of these common sense procedures for avoiding accidental or inadvertent disclosures:

***Measures to Protect PHI***

1. Verbal PHI. Staff members should only discuss PHI with those who are involved in the care of the patient, regardless of physical location. When discussing PHI with patients, staff members should make sure that there are no other persons (including other PRO staff members) in the area that could overhear the discussion. If so, the patient should be brought into a screened area before engaging in discussion.

2. Hard Copy PHI. All paper patient care reports should be stored in safe and secure areas when not in use. No paper records concerning a patient should be left in open bins or on desktops or other surfaces. Only those with a need to have the information for the completion of their job duties should have access to any paper records. Additionally, billing records, including all notes, remittance advices, charge slips or claim forms should not be left out in the open and should be

stored in files or boxes that are secure and in an area with access limited to those who need access to the information for the completion of their job duties.

3. E-PHI. Computer access terminals and other mobile devices should be kept secure. Staff members should be sensitive to who may be in viewing range of the monitor screen and take simple steps to shield viewing of the screen by unauthorized persons. All mobile devices such as laptops, ePCRs and cell phones should remain in the physical possession of the individual to whom they are assigned at all times.

# Pro Policy 1200.13

## Policy 13: Policy on Designated Record Sets

### Purpose

To ensure that PRO patients and their authorized representatives are granted rights regarding Protected Health Information ("PHI") in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), this policy establishes what protected health information ("PHI") at PRO should be accessible to patients as part of a Designated Record Set ("DRS"). Under HIPAA, a DRS includes medical records that are created or used by PRO to make decisions about the patient.

### Scope

This policy applies to all PRO staff members responsible for the designation of PHI into designated record sets and those responsible for fulfilling patient requests pertaining to PHI. All staff members should be familiar with the types of information that will be part of a DRS. Generally, the HIPAA Compliance Officer will be responsible for fulfilling patient requests related to PHI and for ensuring that the correct information is made part of the DRS.

### Procedure

The DRS should only include PHI as defined under HIPAA, and should be comprised of individually identifiable healthcare and billing information created, received, maintained or transmitted by or on behalf of PRO that is used, in whole or in part, by PRO to make decisions about individuals. The HIPAA Compliance Officer shall be the party in charge of designating what information is part of a DRS at PRO and for ensuring that appropriate information is being maintained by PRO in its designated record sets.

***The Designated Record Set at PRO***

1. The DRS at PRO for any requests regarding PHI includes the following records:
    a. Paper or electronic patient care reports ("PCR" or "ePCR") created or received by PRO and supplementary information regarding the patient's condition. This includes any photos, videos, monitor strips, Physician Certification Statements, Refusal of Care forms, Advance Beneficiary Notice of Noncoverage forms, or information from other source used by PRO to treat patients or bill for services.
    b. The electronic claims records or other paper records of submission of actual claims to Medicare or other insurance companies.
    c. Any patient-specific claim and billing information, including responses from insurance payers, such as remittance advice statements, Explanation of Medicare Benefits (EOMBs), charge screens, patient account statements, and signature authorization and agreement to pay documents.
    d. Notices from insurance companies indicating coverage determinations, documentation submitted by the patient, and copies of the patient's insurance card or policy coverage summary, that relate directly to the care of the patient or payment for that care.
    e. Amendments to PHI, or statements of disagreement by the patient requesting the amendment when PHI is not amended upon request, or an accurate summary of the statement of disagreement.

2. The DRS should also include treatment related records created by other parties such as first responder units, assisting ambulance services, air medical services, nursing homes, hospitals, police departments, coroner's offices, etc., that are used by PRO for treatment and payment related purposes.
3. A designated record set should not include:
    a. Quality assurance data collected and maintained for peer review purposes;
    b. Accident reports;
    c. Incident reports;
    d. Duplicate information maintained in other systems;
    e. Data collected and maintained for research;
    f. Information compiled in reasonable anticipation of litigation or administrative action;
    g. Employment records; or
    h. Student records.

# Pro Policy 1200.14

## Policy 14: Policy on News Media Interaction

### Purpose

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") establishes the circumstances under which individuals' protected health information ("PHI") can be disclosed. Generally, PRO may not disclose PHI to the news media without the patient's written express authorization. In addition, state laws may also grant patients additional privacy protections and may enable parties to bring legal action for invasion of privacy or other related causes of action for improper releases of patient information to the news media – sometimes even information that might not qualify as PHI under HIPAA.

This policy establishes consistent guidelines for PRO to follow when dealing with requests from the media so that PRO respects individual privacy rights and complies with applicable federal and state law. This policy will is meant to work in conjunction with PRO's "Action Plan on News Media Interaction." PRO fully respects the right of the public to know about events, but we will provide information to the news media only to the extent that the law allows us and only when it would not infringe on the privacy rights of our patients.

### Scope

This policy applies to all PRO staff members who might come into contact with or who may be contacted by various media outlets. Generally, all requests from the media for any information about an incident involving PRO will be directed to our Public Information Officer to handle. Or, if PRO does not have a designated Public Information Officer, all requests should be directed to our HIPAA Compliance Officer.

### Procedure

***Requests from the News Media***

1. PRO staff members will at all times treat members of the media in a professional manner when a request for information is made.
2. All information requests from the news media received by any PRO staff members shall be directed to the Public Information Officer. Or, if PRO does not have a designated Public Information Officer, all requests from the news media shall be directed to the HIPAA Compliance Officer. Upon receipt of a request for information from the news media, staff members should inform the news media requestor that it is the policy of PRO that all media requests be handled by one official and staff members should provide the media requestor contact information for the Public Information Officer or HIPAA Compliance Officer, as appropriate. Or, the staff member may contact the Public Information Officer or HIPAA Compliance Officer to inform the Officer of the request and request authorization to release information to the media.
3. Staff members other tha PRO's Public Information Officer or HIPAA Compliance Officer are not permitted to release information to the news media, unless authorized or directed by the appropriate Officer to do so.
4. The Public Information Officer or HIPAA Compliance Officer shall use discretion in handling requests from the news media and when deciding whether to release (or permit the release) of information to the media. The Public Information Officer or HIPAA Compliance Officer should

only release information to the media when such release would not violate federal or state laws and when release would not infringe a patient's reasonable expectation to privacy. For example, if PRO transported a high profile member of the community, PRO should probably decline to disclose even general information that does identify the individual to the media since it is likely the patient's identity would be known to anyone hearing the report.

***Releasing Information to the News Media***

1. PRO may not release any PHI to the news media, absent a patient's written, signed authorization. In the event that the patient or the patient's authorized representative signs a HIPAA-compliant authorization form, disclosures of information, including PHI, may be made so long as they are done in accordance with the express terms of the written Authorization. PRO's "Authorization to Use and Disclose Protected Health Information" Form should be used for this purpose.
2. If there is no written authorization from the patient, PRO may only release information that is "de-identified." De-identified information is information that does not identify an individual and there is no reasonable basis to believe that the information can be used to identify a specific individual. PRO may only release the following types of "de-identified" information to members of the media where appropriate:
    a. Name of hospital. PRO may provide the name of the hospital to which patients have been transported. (*Example*: The media calls about "the accident at Third and Main earlier this afternoon." PRO may inform the media that "a patient was transported from the accident scene to ABC Hospital.")
    b. Number of patients. PRO may provide the total number of patients involved in an incident or transported to a facility. PRO may not indicate specifics, such as the type of vehicle a patient was driving or which patient went to a particular facility. (*Example*: PRO may inform the media that "four patients were transported from the fire at the Chemical Factory. Two were taken to County General and two were taken to the Regional Medical Center.")
    c. Age & Gender. PRO may provide the age of a patient and the gender of the patient, unless it could reasonably be used to identify the patient. (*Example*: PRO may inform the media that "a 39 y/o male was transported from the accident on the Interstate.")
    d. Designation of crew members. PRO may state, for example, that one paramedic and two EMTs were involved in caring for the patients involved in a motor vehicle accident. PRO may identify the names of the personnel who responded. (*Example*: PRO may inform the media that "PRO personnel on the scene of the incident included two paramedics and a supervisor and advanced life support was administered.")
    e. Type of Transport. PRO may indicate that a particular call was an emergency and that transportation was facilitated by ambulance or helicopter. (*Example*: "Of the 3 patients on the scene of the incident, one was transported by helicopter to the Trauma Center and two were transported as non-emergency patients to the local hospital emergency department.")

## Pro Policy 1200.15

Policy 15: Action Plan on News Media Interaction

| Step 1: Is the request asking PRO to disclose PHI? | YES | NO |
|---|---|---|
| Upon receipt of a request for information from the news media, the Public Information Officer or HIPAA Compliance Officer shall determine whether the request is asking PRO to disclose PHI. | Go to Step 2 | Go to Step 3 |

Step 2: PRO will not release any PHI to the news media absent a patient's written, signed authorization. The Public Information Officer or HIPAA Compliance Officer may consider asking the patient, or the patient's personal representative, whether they would agree to allow PRO to release the requested PHI to the news media. In the event that the patient or the patient's authorized representative does agree to permit PRO to make the disclosure, the Public Information Officer or HIPAA Compliance Officer shall require the individual to complete and sign PRO's "Authorization to Use and Disclose Protected Health Information" Form to permit the disclosure. PRO may only disclose PHI to the media in strict compliance with what the Authorization states.

Step 3: PRO may release the following types of "de-identified" information to members of the media in accordance with PRO's "Policy on News Media Interaction":

- Name of hospital
- Number of patients
- Age and gender of patients
- Designation of crew members
- Type of transport

# Pro Policy 1200.16

## Policy 16: Policy on Release of PHI to Law Enforcement Without Legal Process

### Purpose

Protected health information ("PHI") may only be released to law enforcement officials under specific and limited circumstances under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). This policy provides consistent guidelines for PRO staff members to follow regarding the release of PHI to law enforcement when the law enforcement official does not serve some type of legal process, such as a summons, subpoena, or warrant, so that staff only release PHI in accordance with HIPAA. This policy will work in conjunction with PRO's "Staff Member Action Plan for Release of PHI to Law Enforcement Without Legal Process."

### Scope

This policy applies to all PRO staff members who may come in contact with law enforcement including field personnel who may encounter law enforcement officials at the scene of an incident and other staff who may be approached by law enforcement directly after an incident. This policy applies to situations where law enforcement is seeking PHI from a staff member and the law enforcement official does not present PRO with legal process, such as a subpoena, summons or warrant. PRO's Policy on Release of Protected Information Pursuant to Warrant, Subpoena, Summons or Administrative Request applies to situations where law enforcement or other parties are seeking information pursuant to legal process.

### Procedure

***General Procedure for Handling Requests***

1. If a staff member of PRO is approached by a law enforcement official and the official makes requests a request for PHI about a patient from the staff member, the staff member should verify the identity of the law enforcement official and ask the official what is the purpose for which the request is being made.
2. If the request is being made for one of the purposes listed in this policy, then the staff member may release the PHI to the law enforcement official, in accordance with this policy. Formal written patient authorization is not required when releasing PHI pursuant to one of the purposes listed in this policy; however, where the patient is readily available and able to consent to the disclosure, verbal consent should be obtained and documented by the staff member before disclosure of PHI is made to the law enforcement official.
3. If the staff member is unsure about whether the release of PHI is proper, the staff member should contact PRO's HIPAA Compliance Officer or an immediate supervisor for guidance. Under no circumstance should any staff member release PHI to law enforcement if the staff member is unsure about the appropriateness of the disclosure.
4. If the request for PHI does not fall under one of the purposes listed in this policy, the staff member should inform the law enforcement officer that s/he is not permitted under HIPAA to release the information. The staff member may inform the law enforcement official of the following two options:
    1. The law enforcement official may obtain legal process, such as a warrant, summons, or subpoena, to obtain the information from PRO.

2. The law enforcement official may obtain the information directly from the patient if the patient is stable and willing to speak with the official. Staff members should only provide this option to a law enforcement official when doing so would not impede patient care and where the patient is willing to speak with the official. For a stable patient, the staff member should first consult with the patient to determine whether the patient is willing to speak with the official. If the patient declines to speak with the official, the staff member should inform the enforcement official.

5. Staff members should record, at a minimum, the following information about all law enforcement requests that are unaccompanied by legal process:
    1. The name of the law enforcement official;
    2. The date and time of the request;
    3. The purposes for which the request was made (if provided);
    4. What information the law enforcement official requested;
    5. Whether the patient was consulted about the request and the patient's response;
    6. Whether the HIPAA Compliance Officer or other individual at PRO was consulted about the request;
    7. Whether the law enforcement official made any representations to PRO;
    8. Whether PHI was released and what PHI was released; and
    9. The reason(s) why the PHI was released.

Purposes for Which Disclosure Can Be Made to Law Enforcement Without Legal Process

***Disclosures of PHI Required by State Reporting Law***

1. Massachusetts law requires that PRO staff members report the following types of incidents to law enforcement agencies in Massachusetts:
2. If there is any doubt regarding whether or not Massachusetts requires reporting of a particular injury or incident, the staff member should contact a supervisor for a list of incidents that must reported under Massachusetts law.

***Disclosures of PHI to Locate or Identify a Suspect, Material Witness, Fugitive or Missing Person***

1. PHI may be disclosed to law enforcement for purpose of locating or identifying a ***suspect, material witness, fugitive*** or ***missing person*** only upon request of a law enforcement official. The disclosure may not be initiated by PRO.
2. If a law enforcement official indicates to a staff member that they need PHI about an individual to identify or locate a ***suspect***, ***material witness***, ***fugitive*** or ***missing person***, the staff member should ask the law enforcement official to confirm that the *sole* purpose of the request is to locate or identify one of the listed individuals. If the law enforcement official already knows who the individual is and where the individual is located, then the staff member should not proceed to disclose PHI for this purpose.
3. Although no formal written request is required from law enforcement, the staff member should ask that the PHI request be documented in writing, preferably on the law enforcement department's letterhead. In the absence of a written request from the law enforcement agency, the staff member should, at a minimum, document that the law enforcement officer verified that the PHI was needed to identify or locate a ***suspect, material witness, fugitive*** or ***missing person***.

4. If the staff member is satisfied that law enforcement has made a good faith representation that the information requested is needed to locate or identify a ***suspect, fugitive, material witness***, or ***missing person***, then the staff member may disclose only the following PHI about that individual to the official:- Name

   – Address

   – Date of birth

   – Place of birth

   – Social Security Number

   – Blood type

   – Type of injury

   – Date of treatment

   – Time of treatment

   – Description of distinguishing physical characteristics (i.e. weight, hair color, eye color, gender, facial hair, scars and tattoos)

***Disclosing PHI About Crime Victims***

1. PHI about crime victims may be disclosed to law enforcement only upon request of a law enforcement official. The disclosure may not be initiated by PRO.
2. If a law enforcement officer requests PHI about an individual who may be the victim of a crime, PRO staff members should first discern whether the individual is in fact a victim of a crime. Victims of a crime may include motor accident victims because often a summary or misdemeanor offense is involved (like when the accident is the result of the driver of another vehicle violating traffic laws). In many cases, the determination that a patient is or may be a crime victim can be inferred from the circumstances and the presence of law enforcement at the scene.
3. PRO may disclose PHI about a crime victim to a law enforcement official if the individual agrees to the disclosure. If the patient is conscious and alert, and it would not impede the provision of care, the staff member should ask the patient if it is acceptable to disclose the PHI to law enforcement. If the patient does not consent to the disclosure, then PHI should not be disclosed and law enforcement should be informed of that fact. If the victim does consent to the disclosure, the PHI may be released in accordance with the patient's wishes. The consent may be verbal, but it should be documented on a patient care report or other document.
4. If the patient is unable to consent, due to incapacity or other reason, the staff member should ask law enforcement if they can wait until the patient is able to consent to the release of the PHI. If the law enforcement official represents that waiting until the patient is capable of agreeing to the disclosure would compromise an immediate law enforcement activity, then PHI may be disclosed to law enforcement provided the following conditions are met:
    1. The staff member, in the exercise of professional judgment, determines that disclosure would be in the best interests of the crime victim;

2. The law enforcement officer needs the information to determine whether a violation of law has occurred; and
3. The law enforcement officer represents that the information requested is not intended to be used against the crime victim.

Representations from law enforcement may be verbal and should be documented in a patient care report or other document.

***Disclosing PHI Regarding Victims of Abuse, Neglect, or Domestic Violence***

1. If law enforcement makes a request for PHI regarding someone who a PRO staff member reasonably believes to be the victim of violence or abuse, PRO may release PHI to law enforcement if the patient agrees to the disclosures. The staff member should first ask the patient for his/her consent to release the information. If the patient does not consent to the disclosure, no PHI should be provided to law enforcement and law enforcement should be informed of this fact. If the individual agrees to the disclosure of PHI, the staff member may give the PHI to law enforcement in accordance with the patient's consent. This consent can be verbal but it should be documented on the patient care report.
2. If the individual is unable to consent to the disclosures due to incapacity, mental condition, etc., and the laws of Massachusetts expressly authorize reporting of this type of information to law enforcement, PRO staff members may release PHI to law enforcement provided that either of the following conditions are met:
    1. The staff member, in the exercise of professional judgment, believes that the disclosure is necessary to prevent serious harm to the patient or other potential victims; or
    2. Law enforcement assures the staff member that the PHI will not be used against the victim and represents that an immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.
3. Representations from law enforcement may be verbal and should be documented in a patient care report by the staff member along with all details regarding the disclosure including the identity of the requestor, the purpose of the request, the date and time of the request, and the PHI released about the victim.
4. If PRO discloses PHI without the patient's consent because the patient was unable to consent, the HIPAA Compliance Officer must contact the patient and alert them of the disclosure, unless PRO believes contacting the patient will only put the patient at greater risk.

***Disclosing PHI Regarding Decedents***

1. PHI can be released to law enforcement about decedents without a request for PHI from a law enforcement official (*i.e.,* PRO may initiate this type of disclosure).
2. PRO staff members may disclose limited PHI to law enforcement about an individual who has died when staff members have a reasonable, good faith belief that the death may have resulted from criminal conduct. The staff member does not necessarily have to come to a legal conclusion, or know with complete certainty, that the death resulted from a crime. This includes any type of crime.

3. Disclosure regarding suspected victims of a crime should be limited to basic facts about the victim and the circumstances of the death.

***Disclosing PHI to Report a Crime on PRO's Premises***

1. PRO may initiate this type of disclosure to law enforcement absent a request from a law enforcement official.
2. PRO staff members may disclose to law enforcement any PHI that staff members in good faith believe constitutes evidence of a crime committed on PRO's premises. PRO's premises include the station house, headquarters, parking lot, the ambulance, etc.
3. Disclosure of PHI to report a crime on the premises should be limited to information that is necessary to alert law enforcement about the crime and to describe the crime to law enforcement.

***Disclosing PHI to Report a Crime in an Emergency***

1. PRO may initiate this type of disclosure to law enforcement absent a request from a law enforcement official.
2. PRO staff members may disclose PHI to law enforcement when they believe it is necessary to alert law enforcement to:

   – The commission of a crime- The nature of a crime

   – The location of the crime

   – The location of a crime victim

   – The identity, description, and location of the perpetrator of a crime

3. Disclosures of PHI to report a crime in an emergency should be limited to necessary information about the nature of the crime and information about the suspect(s).

***Disclosure of PHI to Avert a Serious Threat to Health or Safety***

1. PRO may initiate this type of disclosure to law enforcement absent a request from a law enforcement official.
2. PRO staff members may disclose PHI to avert a serious threat to health or safety so long as a staff member believes that the disclosure is necessary to:
    1. Avert a serious and imminent threat to a person's safety or the public at large;
    2. Identify or apprehend an individual because that individual admitted to participating in a violent crime that may have caused serious harm to someone; or
    3. Identify or apprehend someone who escaped from a correctional institution or from lawful custody.
3. Disclosures of PHI to prevent or lessen a serious and imminent threat to the health or safety should only be made to alert persons who are reasonably able to prevent or lessen the threat.
4. Disclosures of PHI to prevent or lessen a serious threat to health or safety should be limited to necessary information to prevent or lessen the threat, and necessary information about the individual who poses the threat.

# Pro Policy 1200.17

## Policy 17: Staff Member Action Plan for Release of PHI to Law Enforcement Without Legal Process

<table>
<tr><td colspan="3">Step 1: If the request comes from law enforcement, verify the identity of the law enforcement official and ask the official what is the purpose for which the request is being made.</td></tr>
<tr><td>Step 2: Is the law enforcement officer requesting information for one of the law enforcement purposes listed in this action plan?</td><td>NO<br><br>Go to Step 3</td><td>YES<br><br>You may release the PHI in accordance with the corresponding guidance for each purpose, listed in the column directly across from the stated purpose. Formal written patient authorization is not required when releasing PHI pursuant to one of the purposes listed in this policy. But, if the patient is readily available and able to consent to the disclosure, verbal consent should be obtained and documented before disclosure of PHI is made to the law enforcement official. In addition, you should record, at a minimum, the following information about all law enforcement requests that are unaccompanied by legal process:<br>· The name of the law enforcement official;<br>· The date and time of the request;<br>· The purposes for which the request was made (if provided);<br>· What information the law enforcement official requested;<br>· Whether the patient was consulted about the request and the patient's response;<br>· Whether the HIPAA Compliance Officer or other individual at PRO was consulted about the request;<br>· Whether the law enforcement official made any representations to PRO;<br>· Whether PHI was released and what PHI was released; and<br>· The reason(s) why the PHI was released.</td></tr>
</table>

| | |
|---|---|
| Required by State Reporting Law<br><br>The information that the law enforcement officer is asking for is required to be reported to law enforcement under state law (*e.g.,* animal bites, gunshot wounds, burn injuries, out-of hospital deaths, vehicle accidents, etc.). | Required by State Reporting Law<br><br>You may release any PHI that is necessary to comply with state reporting law and should track the disclosure on a patient care report or other form and inform the patient about the disclosure, whenever possible. |
| Identify or Locate a Suspect, Material Witness, Fugitive, or Missing Person<br><br>The information is needed by law enforcement for the sole purpose of identifying or locating a suspect, material witness, fugitive, or missing person. | Identify or Locate a Suspect, Material Witness, Fugitive, or Missing Person<br><br>You may release only the following types of PHI about the individual to law enforcement:<br><br>Name; Address; *Date of Birth; Place of Birth; Social Security Number; Blood Type; Type of Injury; Date of Treatment; Time of Treatment; A Description of Distinguishing Physical Characteristics*. |
| Crime Victims<br><br>The information is needed by law enforcement about a person who is or who is suspected by the law enforcement officer to be the victim of a crime. | Crime Victims<br><br>You should first ask whether the victim agrees to the disclosure and if the victim refuses, the PHI should not be released and the officer should be informed that s/he may speak with the victim directly. If the patient agrees, information may be disclosed pursuant to the patient's wishes and the agreement should be documented along with the disclosure. If the patient is unable to agree to the disclosure because he/she is incapacitated or some other reason and the law enforcement official represents that waiting until the patient is capable of agreeing to the disclosure would compromise an immediate law enforcement activity, then you may release the PHI requested provided all the following conditions are met:<br><br>· You determine that disclosure would be in the best interests of the victim; |

| | |
|---|---|
| | · The officer needs the information to determine whether a violation of law has occurred; and<br>· The law enforcement officer represents that the information requested is not intended to be used against the crime victim and you document that representation. |
| -<br>Death from Criminal Activity<br><br>You need to disclose PHI to law enforcement regarding a decedent because it appears that the decedent died as a result of criminal conduct. | -<br>Death from Criminal Activity<br><br>You must first have a reasonable, good faith belief that that the individual's death resulted from criminal conduct. This does not require a legal conclusion and the death may have been the result of any criminal conduct. You should only release information that is necessary to alert law enforcement about the death, such as the identity of the patient and basic facts about the circumstances of the death. |
| -<br>Crime on Premises<br><br>You need to disclose PHI to report a crime that occurred on the premises of PRO or in one of our vehicles. | -<br>Crime on Premises<br><br>You may disclose PHI to law enforcement if you believe in good faith the PHI constitutes evidence of criminal conduct on the premises of PRO's station house, headquarters, parking lot, or any vehicle. The information should be limited to basic information about the patient and circumstances about the crime. |

| | |
|---|---|
| Reporting Crime in Emergency<br><br>You need to disclose PHI to report a crime in an emergency. | Reporting Crime in Emergency<br><br>You may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement to:<br><br>· The commission and nature of a crime;<br>· The location of the crime; and<br>· The identity, description, and location of the perpetrator of such crime. |
| To Avert a Serious Threat to Health or Safety<br><br>You need to disclose PHI to someone who is able to prevent or lessen a serious threat to health or safety. | To Avert a Serious Threat to Health or Safety<br><br>You may disclose PHI to someone who is able to prevent or lessen a threat to health or safety if you believe it is necessary to do so in order to:<br><br>· Avert a serious and imminent threat to a person's safety or the public at large;<br>· Identify or apprehend an individual because that individual admitted to participating in a violent crime that may have caused serious harm to someone; or<br>· Identify or apprehend someone who escaped from a correctional institution or from lawful custody.<br><br>Disclosures of PHI to prevent or lessen a serious threat to health or safety should be limited to necessary information to prevent or lessen the threat, and necessary information about the individual who poses the threat. |

Step 3:

If the request for PHI does not fall under one of the purposes listed in this action plan, you should inform the law enforcement official you are not permitted under HIPAA to release the information. You may inform the law enforcement official of the following two options:

· The law enforcement official may obtain legal process, such as a warrant, summons, subpoena or administrative request to obtain the information from PRO.

· The law enforcement official may obtain the information directly from the patient if the patient is stable and willing to speak with the official. You should only provide this option to a law enforcement official when doing so would not impede patient care and where the patient is willing to speak with the official. You should first consult with the patient to determine whether the patient is willing to speak with the official. If the patient declines to speak with the official, you should inform the enforcement official.

# Pro Policy 1200.18

## Policy 18: Policy on Release of PHI to Law Enforcement With Legal Process

### Purpose

Protected health information ("PHI") may be released pursuant to valid legal process under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). This policy provides guidelines for PRO regarding the release of PHI pursuant to court orders, summonses, subpoenas, warrants, administrative requests, and discovery requests (collectively referred to in this policy as "legal process"), so that PRO only releases PHI in accordance with HIPAA and as required by state law. This policy will work in conjunction with PRO's HIPAA Compliance Officer Action Plans on "Requests for PHI from Attorneys," "Administrative Requests for PHI from Government Agencies," and "Court-Ordered Requests for PHI."

### Scope

This policy applies to all PRO staff members who may receive or respond to requests for PHI accompanied by legal process. These requests typically occur after a call is completed and are generally served on staff at PRO's station in person or through the mail. Generally, all such requests will be directed to and handled by the HIPAA Compliance Officer.

### Procedure

***General Procedure for Handling Requests***

PRO is permitted by HIPAA, and may be required by Massachusetts law and federal law, to furnish requested PHI to certain parties pursuant to a valid legal process.

If PRO receives a request for PHI accompanied by legal process, the request shall be directed to the HIPAA Compliance Officer.

The HIPAA Compliance Officer shall first determine whether the request is: (a) a court order or a court-ordered subpoena, summons or warrant ("SSW"); (b) an administrative request; or (c) a subpoena, discovery request, or other legal process issued by an attorney. When determining what type of request has been received, the HIPAA Compliance Officer shall look to the issuer of the request (*i.e.*, who the requesting party is) and keep in mind the following guidelines:

1. Court orders and court-ordered SSWs are issued by courts, grand juries, and administrative tribunals and signed by a judge or other judicial officer.

1. Administrative requests are issued by a federal, state, or local administrative agency such as a department of health, a law enforcement agency, or other similar type of agency. Administrative agencies are permitted to issue "administrative" warrants, subpoenas, summonses or other similar type requests for information. These documents are likely to be signed by a high level official from the requesting administrative agency.

1. Attorneys may issue subpoenas and discovery requests. These requests can usually be distinguished from other types of "official" court-ordered or administrative requests because they are signed by an attorney, not a judge, judicial officer or administrative official.

When in doubt, the HIPAA Compliance Officer should solicit the assistance of legal counsel in determining what type of request was received.

Patient authorization is not required when releasing PHI pursuant to a request for PHI accompanied by legal process. However, patients may need to be notified about certain requests in accordance with this policy before PHI is released.

All disclosures of PHI pursuant to requests accompanied by legal process must be documented by the HIPAA Compliance Officer in PRO's "Accounting Log for Disclosures of PHI" and a copy of the request shall be maintained with that log in the patient file, along with other information required by this policy.

***Responding to Court-Ordered Requests***

If the HIPAA Compliance Officer determines that the request is a court order or a court-ordered SSW, the HIPAA Compliance Officer shall first verify that the request has been signed by a judge or other judicial officer of a court, grand jury, or administrative tribunal. If the request has not been signed by a judge or judicial officer, the HIPAA Compliance Officer shall send the requestor a letter stating that PRO will not disclose any PHI until PRO receives a court order or court-ordered SSW that is signed by the appropriate party.

If the request is signed by a judge or judicial officer, PRO may disclose ONLY the information that is specifically requested by the court order or court-ordered SSW. For example, the HIPAA Compliance Officer should not simply turn over a copy of all records (including records relating to prior transports and billing records) if the request asks PRO to "provide any treatment records about John Smith from April 15, 2013." However, if the request asks PRO to provide "any and all records pertaining to John Smith," then PRO must generally provide all PCRs, all billing records, and any other information maintained about the patient. The HIPAA Compliance Officer shall also contact the issuer of the request whenever it is unclear what PHI PRO is required to disclose. If necessary, the HIPAA Compliance Officer shall ask that the requester re-issue a more specific request.

The HIPAA Compliance Officer shall retain a copy of the court-ordered request and document the name of the requesting party, the date of the request, the date of disclosure, and the PHI that was disclosed.

***Responding to Administrative Requests from Government Agencies***

If the HIPAA Compliance Officer determines that a request for PHI qualifies as an administrative request (including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process) issued by a federal, state, or local government agency, the HIPAA Compliance Officer should first determine whether the agency has the authority to make the request and to receive the PHI requested. The HIPAA Compliance Officer should look to any statutory or regulatory authority cited in the request and consult with legal counsel when making this determination. If the HIPAA Compliance Officer determines that the agency does not have the legal authority to request and receive the PHI requested, the HIPAA Compliance Officer shall send the requestor a letter stating that PRO will not disclose any PHI until the agency provides PRO with a statement citing appropriate legal authority to request and receive the PHI requested.

If the HIPAA Compliance Officer determines that the agency is authorized by law to make the request, the HIPAA Compliance Officer must then verify that:

1. The PHI sought by the request is relevant and material to a legitimate law enforcement inquiry;

1. The request is specific and limited in scope to the extent reasonable and practicable in light of the purpose for which the PHI is sought; and

1. De-identified information could not reasonably be used.

The HIPAA Compliance Officer should look to the administrative request to determine whether these conditions are clearly met. If it is not clear from the administrative request that all three of the above-listed conditions are met, then the HIPAA Compliance Officer shall contact the administrative agency who issued the request and inform the agency that PHI will not be released until PRO receives written assurances from the requestor that the conditions are met.

If the HIPAA Compliance Officer determines that the above-listed conditions are met, the HIPAA Compliance Officer may release ONLY the PHI that the administrative request asks for. The HIPAA Compliance Officer shall also contact the issuer of the request whenever it is unclear what PHI PRO is required to disclose. If necessary, the HIPAA Compliance Officer shall ask that the requester re-issue a more specific request.

The HIPAA Compliance Officer shall retain a copy of the administrative request as well as any assurances, and document: the name of requesting party; the date of the request; the date of disclosure; and the PHI that was disclosed.

***Responding to Requests from Attorneys***

If the HIPAA Compliance Officer determines that the request is a subpoena, discovery request, or other legal process from an attorney (that is not accompanied by an official order from a court, grand jury or administrative tribunal), the HIPAA Compliance Officer shall first verify that the original subpoena, discovery request, or other legal process is enclosed with the request. References to a subpoena or other document in the request are not sufficient. If the original legal process has not been provided to PRO, the HIPAA Compliance Officer shall send the requestor a letter stating that PRO will not disclose any PHI until the original process has been provided.

Then, the HIPAA Compliance Officer shall verify that "satisfactory written assurances" have been provided to PRO by the requestor. This means that PRO must receive written documentation from the attorney requesting the PHI that demonstrates <u>either</u> of the following:

1. The attorney requesting the PHI made a good faith attempt to provide written notice to the patient that included information about the litigation or proceeding <u>and</u> the PHI request and such notice was sufficient to permit the individual the opportunity to raise an objection to the court or administrative tribunal. Additionally, the time for the patient to raise objections to the court or administrative tribunal has elapsed, and either: (i) no objections were filed; or (ii) all objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution. Documentation may include, for example, a copy of the notice mailed to the individual that includes instructions for raising an objection with the court and the deadline for doing so, and a written statement or other documentation demonstrating that no objections were raised or all objections raised were

resolved and the request is consistent with the resolution. To the extent that the subpoena or other request itself demonstrates the above elements, no additional documentation is required;

OR

1. The parties to the dispute giving rise to the request for PHI have agreed to a "qualified protective order" and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or the attorney seeking the PHI has requested a qualified protective order from such court or administrative tribunal. A "qualified protective order" is an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that: (i) prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and (ii) requires the return of the PHI or destruction of the PHI (including all copies made) at the end of the litigation or proceeding. Documentation may include, for example, a copy of the qualified protective order that the parties have agreed to and documentation or a statement that the order was presented to the court, or a copy of the motion to the court requesting a qualified protective order.

If all written assurances have not been provided to PRO, the HIPAA Compliance Officer shall send the requestor a letter stating that PRO will not disclose any PHI until the proper written assurances have been provided.

If the required satisfactory written assurances have been provided to PRO, then the HIPAA Compliance Officer may disclose PHI as requested in the subpoena or other legal process. The HIPAA Compliance Officer shall ONLY disclose the PHI that has been requested in the document. The HIPAA Compliance Officer shall also contact the issuer of the request whenever it is unclear what PHI PRO is required to disclose. If necessary, the HIPAA Compliance Officer shall ask that the requester re-issue a more specific request.

The HIPAA Compliance Officer shall retain a copy of the request from the attorney as well as the satisfactory written assurances from the attorney in the patient file. The HIPAA Compliance Officer shall also document the name of requesting party, the date of the request, the date of disclosure, and the PHI that was disclosed.

## Pro Policy 1200.19

Policy 19: HIPAA Compliance Officer Action Plan for Court-Ordered Requests for PHI

| | | |
|---|---|---|
| | | NO |
| Step 1: Is the court order or a court-ordered subpoena, summons or warrant ("SSW") signed by a judge or other judicial officer of a court, grand jury or administrative tribunal? | YES<br><br>Go to Step 2 | The HIPAA Compliance Officer should deny the request in writing stating that a court order or court-ordered SSW signed by a judge or judicial officer must be provided to |

PRO before the request will be considered.

Step 2: If the request is signed by a judge or judicial officer, PRO may disclose ONLY the information that is specifically requested by the court order or court-ordered SSW. The HIPAA Compliance Officer shall also contact the issuer of the request whenever it is unclear what PHI PRO is required to disclose. If necessary, the HIPAA Compliance Officer shall ask that the court, grand jury or administrative tribunal re-issue a more specific request. The HIPAA Compliance Officer shall retain a copy of the court-ordered request in the patient file, track the disclosure in an accounting log, and document: the name of requesting entity; the date of the request; the date of disclosure and the PHI that was disclosed.

# Pro Policy 1200.20

Policy 20: HIPAA Compliance Officer Action Plan for Administrative Requests for PHI from Government Agencies

PRO HIPAA Compliance Officer Action Plan:

Administrative Requests for PHI from Government Agencies

| | | |
|---|---|---|
| Step 1: Does the federal, state, or local government agency have the authority to make the administrative request (an administrative request can include an administrative subpoena, summons, civil or other authorized investigative demand or similar process)? The HIPAA Compliance Officer should look to any statutory or regulatory authority cited in the request and consult with legal counsel when making this determination. | YES<br><br>Go to Step 2 | NO<br><br>The HIPAA Compliance Officer should deny the request in writing stating that proper legal authority, demonstrating that the agency has the right to request and receive the PHI, must be provided to PRO by the administrative agency before the request will be considered. |
| Step 2: Is it clear from the request that all 3 conditions below are satisfied?<br><br>1. The PHI sought by the request is relevant and material to a legitimate law enforcement inquiry;<br><br>2. The request is specific and limited in scope to the extent reasonable practicable in light of the purpose for which the PHI is sought; and<br><br>3. De-identified information could not reasonably be used? | YES<br><br>Go to Step 3 | NO<br><br>The HIPAA Compliance Officer should send the requestor a letter stating that PRO will not disclose any PHI until the administrative agency certifies in writing that the three conditions have been met. |
| Step 3:<br><br>The HIPAA Compliance Officer shall ONLY disclose the PHI that has been requested in the administrative request. The HIPAA Compliance Officer shall also contact the issuer of the request whenever it is unclear what PHI PRO is required to disclose. If necessary, the HIPAA Compliance Officer shall ask the requesting agency to re-issue a more specific request. The HIPAA Compliance Officer shall | | |

retain a copy of the administrative request as well as any written assurances in the patient file. The HIPAA Compliance Officer shall also track the disclosure in an accounting log and document: the name of requesting agency; the date of the request; the date of disclosure and the PHI that was disclosed.

# Pro Policy 1200.21

Policy 21: HIPAA Compliance Officer Action Plan for Attorney-Issued Subpoenas and Discovery Requests

| | | |
|---|---|---|
| Step 1: Does the request contain the original subpoena, discovery request, or other legal process? References to a subpoena or other document in the request letter are not sufficient. | YES<br><br>Go to Step 2 | NO<br><br>The HIPAA Compliance Officer should deny the request in writing stating that the original subpoena, discovery request, or other legal process must be provided to PRO before PRO will consider the request. |
| Step 2: Does the request seeking PHI also contain "satisfactory written assurances?" In order to contain satisfactory written assurances, the request must include documentation that demonstrates either of the following:<br><br>· The attorney requesting the PHI made a good faith attempt to provide written notice to the patient that included information about the litigation or proceeding and the PHI request, and such notice was sufficient to permit the individual the opportunity to raise an objection to the court or administrative tribunal. Additionally, the time for the patient to raise objections to the court or administrative tribunal has elapsed, and either: (i) no objections were filed; or (ii) all objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution. Documentation may include, for example, a copy of the notice mailed to the individual that includes instructions for raising an objection with the court and the deadline for doing so, and a written statement or other documentation demonstrating that no objections were raised or all objections raised were resolved and the request is consistent with the | YES<br><br>Go to Step 3 | NO<br><br>The HIPAA Compliance Officer should send the requestor a letter stating that PRO will not disclose any PHI until the proper satisfactory written assurances have been provided to PRO. |

| | | |
|---|---|---|
| resolution. To the extent that the subpoena or other request itself demonstrates the above elements, no additional documentation is required;<br><br>OR<br><br>· The parties to the dispute giving rise to the request for PHI have agreed to a "qualified protective order" and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or the attorney seeking the PHI has requested a qualified protective order from such court or administrative tribunal. A "qualified protective order" is an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that: (i) prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and (ii) requires the return of the PHI or destruction of the PHI (including all copies made) at the end of the litigation or proceeding. Documentation may include, for example, a copy of the qualified protective order that the parties have agreed to and documentation or a statement that the order was presented to the court, or a copy of the motion to the court requesting a qualified protective order. | | |
| Step 3:<br><br>The HIPAA Compliance Officer shall ONLY disclose the PHI that has been requested in the subpoena. The HIPAA Compliance Officer shall also contact the issuer of the request whenever it is unclear what PHI PRO is required to disclose. If necessary, the HIPAA Compliance Officer shall ask the requesting agency to re-issue a more specific request. The HIPAA Compliance Officer shall retain a copy of the request from the attorney as well as the satisfactory written assurances in the patient file. The HIPAA Compliance Officer shall also track the disclosure in an accounting log and document: the name of requesting party; the date of the request; the date of disclosure and the PHI that was disclosed. | | |

# Pro Policy 1200.22

## Policy 22: Policy on Breaches of Unsecured PHI

### Purpose

Under the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") PRO has an obligation, following the discovery of a breach of unsecured protected health information ("PHI"), to notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed. PRO also has an obligation to notify the Department of Health and Human Services ("HHS") of all breaches. In some cases, PRO must notify media outlets about breaches of unsecured PHI. This policy details how PRO will handle and respond to suspected and actual breaches of unsecured PHI.

### Scope

This Policy applies to all PRO staff members who come into contact with PHI. All suspected breach incidents shall be brought to the attention of the HIPAA Compliance Officer and the HIPAA Compliance Officer shall investigate each incident and initiate the appropriate response to the incident.

### Procedure

***Breach Defined***

A breach is the acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

An acquisition, access, use, or disclosure of PHI created, received, maintained or transmitted by PRO that is not permitted by HIPAA is presumed to be a breach unless PRO demonstrates that there is a low probability that the PHI has been compromised based on a "risk assessment" of at least the following factors:

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

1. The unauthorized person who used the PHI or to whom the disclosure was made;

- Whether the PHI was actually acquired or viewed; and

1. The extent to which the risk to the PHI has been mitigated.

"*Unsecured protected health Information"* is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS for securing PHI – available on HHS's website at: http://www.hhs.gov/ocr/privacy. Generally, PHI is "unsecured" if it is not encrypted by strong encryption technology or if it has not been properly destroyed. If the PHI is able to be used, read, or deciphered it is "unsecured."

A breach does not include any of the following:

1. Unintentional acquisition, access, or use of unsecured PHI by a staff member at PRO or someone acting under the authority of PRO if the acquisition, access, or use was made in good faith and within that individual's scope of authority, so long as the information was not further used or disclosed in violation of HIPAA.

1. Any inadvertent disclosure of PHI by a PRO staff member who is generally authorized to access PHI to another person at PRO who is generally authorized to access PHI, so long as the information received as a result of such disclosure was not further used or disclosed in violation of HIPAA.

1. A disclosure of PHI where PRO has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

***Reporting a Suspected Breach Incident***

All PRO staff members are responsible for immediately reporting a suspected breach incident to a supervisor or the HIPAA Compliance Officer. PRO staff members shall report all known and suspected HIPAA violations.

The HIPAA Compliance Officer will notify management about the suspected incident.

The HIPAA Compliance Officer shall document the date that the suspected breach of unsecured PHI occurred (if known) and the date(s) on which the supervisor and the HIPAA Compliance Officer were notified about the incident.

***Investigating a Suspected Breach Incident***

The HIPAA Compliance Officer shall then initiate an investigation to determine whether an actual breach has occurred and what actions, if any, are necessary.

The HIPAA Compliance Officer shall interview all necessary parties who may have information about the incident. The staff member who reported the suspected incident and other members with knowledge of the incident should be asked to complete PRO's "Internal Breach Incident Reporting Form." Staff members should be required to convey all information that they know about the incident and to cooperate in any subsequent investigation regarding the incident.

After gathering all available information about the incident, the HIPAA Compliance Officer shall conduct an analysis to determine whether an actual breach of unsecured PHI occurred. PRO shall consult with legal counsel whenever necessary in making this determination. The HIPAA Compliance Officer shall utilize PRO's "HIPAA Compliance Officer Action Plan: Breach Analysis Steps" in making this determination.

If the Compliance Officer determines that a breach of unsecured PHI has not occurred, the reasons behind that conclusion shall be thoroughly documented.

If the HIPAA Compliance Officer determines that a breach of unsecured PHI has occurred, the reasons behind that conclusion shall be thoroughly documented and the HIPAA Compliance Officer shall proceed to notify all necessary parties in accordance with this policy.

***Breach Notification to Affected Individuals***

Following the discovery of a breach of unsecured PHI, PRO will notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach. The HIPAA Compliance Officer shall be the party who is primarily responsible to make proper notice, in consultation with PRO management.

A breach shall be treated as discovered by PRO as of the first day on which the breach is known, or, by exercising reasonable diligence would have been known to PRO or any person, other than the person committing the breach, who is a staff member or agent of PRO.

PRO shall provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

If a law enforcement official states to PRO that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, PRO shall:

1. Delay notification for the time period specified by the official if the statement is in writing and specifies the time for which a delay is required; or

1. If the notice is a verbal statement, delay notification temporarily, and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time. If the statement is made orally, the HIPAA Compliance Officer shall document the statement, including the identity of the official making the statement.

1. PRO shall provide written notification, in plain language, by first-class mail to each affected individual at the last known address of each individual. If the affected individual agreed to receive electronic notice of breaches, PRO may provide notice by electronic mail. The notification may be provided in one or more mailings as information becomes available.

1. The HIPAA Compliance Officer shall utilize PRO's "Individual Notice of Breach of Unsecured PHI" when sending notice to affected parties. The Notice shall include, to the extent possible:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

1. A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, or other types of information were involved);

1. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

1. A brief description of what PRO is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

1. Contact procedures for individuals to ask questions or learn additional information about the incident from PRO. These contract procedures shall include a toll-free telephone number and an e-mail address to reach PRO's HIPAA Compliance Officer.

If the HIPAA Compliance Officer determines that affected individuals need to be contacted immediately to protect them from potential harm, the HIPAA Compliance Officer shall contact those individuals by telephone or other means as soon as possible. PRO shall still send written notice to these individuals about the incident.

If PRO knows that any affected individual is deceased and PRO has the address of the next of kin or personal representative of the individual, PRO shall provide written notification by first class mail to either the next of kin or personal representative.

If PRO has insufficient or out-of-date contact information for any affected individuals, PRO shall use a substitute form of notice that, in the informed opinion of the HIPAA Compliance Officer, will reach the individual. Substitute notice is not required in cases where there is insufficient or out-of-date contact information for the next of kin or personal representative of a deceased individual. Substitute notice will be provided in the following manner:

1. If there is insufficient or out-of-date contact information for fewer than 10 affected individuals, then substitute notice may be provided by an alternative form of written notice such as placing a notice in the newspaper, calling the patient, or other means.

1. If there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall: (i) be conspicuously posted on PRO's home page of its website for 90 days, or conspicuous notice in major print or broadcast media in geographic areas where each affected individual likely resides; and (ii) include a toll-free phone number for PRO that remains active for at least 90 days where individuals can learn whether their unsecured PHI may be included in the breach.

***Breach Notification to the Media***

For a breach of unsecured PHI involving more than 500 residents of a single state or jurisdiction, PRO shall notify prominent media outlets serving the state or jurisdiction about the breach. The HIPAA Compliance Officer shall be the party in charge of making such notice and shall make such notification in consultation with PRO management and legal counsel.

Notification to the media shall be made without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.

Notification to the media shall include all information that must be included in individual notice.

***Breach Notification to HHS***

PRO shall notify HHS of all breaches of unsecured PHI in accordance with this policy.

For breaches of unsecured PHI involving 500 or more individuals, PRO shall provide notice to HHS when it provides notice to affected individuals. Notice must be provided in the manner specified on the HHS Website at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/. The HIPAA Compliance Officer shall be responsible for ensuring that such notice is submitted to HHS and must consult management before submitting the information to HHS.

For breaches of unsecured PHI involving less than 500 individuals, PRO shall maintain a log of such breaches and report them to HHS on an annual basis. The HIPAA Compliance Officer shall track these breaches on PRO's "Log for Tracking Breach Incidents." The HIPAA Compliance Officer shall report these breaches to HHS annually, no later than 60 days after the end of the calendar year in which these breaches were discovered. This shall be done in the manner specified on the HHS Website at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/. The HIPAA Compliance Officer shall ensure that the information is submitted to HHS by March 1 of each year and must consult with management before submitting the information to HHS.

***Breach Notification in Accordance with State Law***

The HIPAA Compliance Officer shall also determine, in consultation with legal counsel, whether PRO has any additional breach notification obligations under applicable Massachusetts laws or other state laws.

PRO must look to each state in which an affected individual resides when making this determination and shall consult legal counsel licensed to practice in those states.

***Administrative Requirements***

The HIPAA Compliance Officer shall record and maintain thorough records of all activities related to suspected and actual breach incidents.

In the event of a suspected crime, or other unlawful activity, local, state, or federal law enforcement may need to be notified. That determination will be made by management with recommendation from the HIPAA Compliance Officer. The HIPAA Compliance Officer shall coordinate communications with outside organizations and law enforcement.

PRO will train all members of its staff so that they are able to identify suspected breaches of unsecured PHI and know to report all suspected breaches to the appropriate party immediately.

Staff members who violate this policy will be subject to disciplinary action, up to and including termination.

## Pro Policy 1200.23

Policy 23: HIPAA Compliance Officer Action Plan: Breach Analysis Steps

| | | |
|---|---|---|
| Step 1: Was there an acquisition, access, use or disclosure of PHI that was created, received, maintained, or transmitted by PRO? The HIPAA Compliance Officer shall determine whether PHI was actually involved in the incident, keeping in mind that PHI only includes individually identifiable information that relates to an individual's healthcare or payment for healthcare. | YES<br><br>Go to Step 2 | NO<br><br>There has been no breach of unsecured PHI and breach notification is unnecessary. |
| Step 2: Was the PHI involved in the incident "unsecured?" PHI involved in an incident will be considered to be "unsecured" when it is in electronic form and it is not encrypted in | YES<br>- | NO<br>- |

| | | |
|---|---|---|
| accordance with PRO's "Policy on Encryption and Decryption of e-PHI." | Go to Step 3 | If the HIPAA Compliance Officer determines that the PHI involved in the incident was secured in accordance with PRO's policies on securing hard copy and electronic PHI, then there has been no breach of unsecured PHI and breach notification is unnecessary. |
| Step 3: Was there a HIPAA violation? The HIPAA Compliance Officer must make a determination that there was a violation of the HIPAA Privacy Rule. The incident must involve a use or disclosure that is not permitted by HIPAA. | YES<br><br>Go to Step 4 | NO<br><br>There has been no breach of unsecured PHI and breach notification is unnecessary. |
| Step 4: Did the incident compromise the security or privacy of the PHI involved? To determine whether the incident compromised the security or privacy of the PHI that was potentially breached, the HIPAA Compliance Officer must look to the 4-factors outlined below:<br><br>Factor — Explanation<br><br>1. The nature and extent of the PHI involved — Consider the type and amount of PHI involve the incident involved sensitive information. credit card numbers, social security number information that could be used for identity t fraud more likely compromises the security The same is true for clinical information, esp clinical information (e.g., treatment, medica history information, etc.). | Yes<br><br>Go to Step 5 | NO<br><br>There has been no breach of unsecured PHI and breach notification is unnecessary. |

| | | | |
|---|---|---|---|
| 2. The person who used the PHI or to whom the disclosure was made | Consider whether the person who received the information has obligations to protect the information. For example, other covered entities are obligated to protect PHI that they receive in the same manner as PRO. | | |
| 3. Whether the PHI was actually acquired or viewed | Determine whether the improperly disclosed PHI was returned *before* being accessed for an improper purpose. | | |
| 4. The extent to which the risk to the PHI has been mitigated | Consider whether immediate steps were taken to mitigate the potential harm from the improper use or disclosure of the PHI. | | |
| Step Five: Does a breach exception apply? The HIPAA Compliance Officer must also determine whether one of the breach exceptions outlined in the Breach Notification Rule applies to the incident. If so, there is no reportable breach. The three breach exceptions are:<br><br>· Unintentional Access, Acquisition or Use of PHI. The incident involved *unintentional* access, acquisition or use of PHI by a workforce member of PRO or someone acting under the authority of PRO. The unintentional incident must: (1) be made in good faith; (2) made within the scope of employment; and (3) not result in further improper use or disclosure of PHI.<br><br>· Inadvertent Disclosure to an Authorized Party. Inadvertent disclosure between parties at PRO who are authorized to access PHI is not a breach if the PHI is not further used or disclosed in violation of HIPAA. "Authorized to access PHI" means that the two parties involved in the incident are authorized to access PHI *in general* – not necessarily that they are authorized to access the same type of PHI. | Yes<br><br>PRO does not have to make breach notification. | NO<br><br>PRO must make breach notification in accordance with PRO's "Policy on Breaches of Unsecured Protected Health Information." |

| | | |
|---|---|---|
| · Disclosure Where Retention Was Not Possible. If the HIPAA Compliance Officer can demonstrate that an unauthorized recipient of the improperly disclosed PHI would not reasonably have been able to retain the PHI, this breach exception applies. | | |

# Pro Policy 1200.24

## Policy 24: Policy on Staff Member Access to e-PHI

### Purpose

Under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") PRO is required to ensure that all staff members have appropriate access to e-PHI, and that his or her identity is properly verified before access to PRO's networks, systems and applications containing e-PHI can be obtained. This policy establishes procedures to prevent staff members (including former staff members) who should not have access to e-PHI from obtaining it, and ensures that those who are authorized to have access to e-PHI obtain access in a secure fashion.

### Scope

This policy applies to all PRO staff members who have access to any e-PHI that is created, received, maintained or transmitted by PRO. The HIPAA Compliance Officer shall be responsible for ensuring proper administration of this policy.

### Procedure

***Authority to Access e-PHI***

Staff members seeking access to any network, system, or application that contains e-PHI must satisfy a user authentication mechanism such as unique user identification and password, biometric input, or a user identification smart card to verify their identity and authority to access e-PHI.

Staff members seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and password, or other authentication information.

Staff members should take reasonable steps to ensure that they verify the identity and correct address (digital or physical) of the receiving person or entity prior to transmitting e-PHI. This might include sending a "test email" or calling a party before a fax is sent.

***Unique User Identification***

Any staff member or authorized user that requires access to any network, system, or application that creates, receives, maintains or transmits e-PHI at PRO must be provided with a Unique User Identification Number.

When requesting access to any network, system, or application that creates, receives, maintains or transmits e-PHI at PRO, a staff member or authorized user must supply their assigned Unique User Identification in conjunction with a secure password.

If a staff member or authorized user believes their User Identification has been comprised, they must report that incident to the appropriate supervisor or the HIPAA Compliance Officer immediately.

***Security Password Management***

All staff members must create a password in conjunction with their Unique User Identification to gain access to any network, system or application used to create, receive, maintain or transmit e-PHI at PRO.

A generic User Identification and password may be utilized for access to shared or common area workstations so long as the login provides no access to e-PHI. An additional Unique User Identification and password must be supplied to access networks, systems applications and database systems containing e-PHI at PRO.

Managers of networks, systems, or applications used to create, receive, maintain or transmit e-PHI at PRO must ensure that passwords set by staff members meet the minimum level of complexity described in this policy.

Managers of networks, systems, or applications used to create, receive, maintain or e-PHI are responsible for educating staff members about all password related policies and procedures, and any changes to those policies and procedures.

Password "aging times" (i.e., the period of time a password may be used before it must be changed) must be implemented in a manner commensurate with the criticality and sensitivity of the e-PHI contained within each network, system, application or database.

Staff members are responsible for the proper use and protection of their passwords and must adhere to the following guidelines:

1. Passwords are only to be used for legitimate access to networks, systems, or applications.

1. Passwords must not be disclosed to other staff members or individuals.

1. Staff members must not allow other staff members or individuals to use their password.

1. Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.

1. All passwords used to gain access to any network, system, or application used to access, transmit, receive, or store e-PHI must be of sufficient complexity to ensure that it is not easily guessable.

1. Passwords should be a minimum of eight characters in length.

Passwords should incorporate <u>three</u> of the following characteristics:

1. Any lower case letters (a-z)

1. Any upper case letters (A-Z)

iii. Any numbers (0-9)

1. Any punctuation or non-alphanumeric characters found on a standard ASCII keyboard (! @ # $ % ^ & * ( ) _ – + = { } [ ] : ; " ' | \ / ? < > , . ~ `).

1. Passwords must not include easily guessed information such as personal information, names, pets, birth dates, etc.

1. Passwords must not be words found in a dictionary.

***Emergency Access to e-PHI and PHI***

If a system, network or application contains e-PHI used to provide patient treatment, and the denial or strict access to that e-PHI could inhibit or negatively affect patient care, staff members responsible for electronic information systems must ensure that access to that system is made available to any caregiver in case of an emergency.

***Termination of Access***

1. All supervisors will immediately notify the HIPAA Compliance Officer when a staff member has been separated from service with PRO or when the person no longer is permitted to access e-PHI on PRO's systems, networks, or applications.

1. Staff members' access to PRO's systems, networks and applications containing e-PHI will immediately be disabled on the effective date of the separation or, if still on the staff, the effective date when authorization for access to e-PHI has ended.

1. The staff member will be removed from all information system access lists.

1. The staff member will be removed from all user accounts.

1. The staff member will turn in all keys, tokens, or access cards that allow access to the information system.

1. The "Staff Member Termination Checklist" will be completed by the supervisor the last day of the staff member's authorized access.

# Pro Policy 1200.25

## Policy 25: Policy on Contingency Planning

### Purpose

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires PRO to implement a policy to ensure that we effectively protect the integrity of protected health information ("PHI") that we hold in the event of an emergency. This policy ensures that our response to an emergency or other occurrence that threatens or damages our computer, electronic, or other information systems is appropriate and provides for the contingencies necessary to protect and preserve PHI in accordance with the HIPAA.

### Scope

This policy contains procedures for protecting the integrity of PHI (including e-PHI) and other essential patient information, billing and business information, and confidential information in the event of an emergency or other occurrence (i.e., fire, vandalism, system failure and natural disaster). The HIPAA Compliance Officer shall oversee the implementation of these procedures.

### Procedure

***Applications and Data Criticality Analysis***

PRO will assess the relative criticality of specific applications and data within the company for purposes of developing its Data Backup Plan, its Disaster Recovery Plan and its Emergency Mode Operation Plan.

The assessment of data and application criticality should be conducted periodically and at least annually as part of the Security Risk Analysis to ensure that appropriate procedures are in place for data and applications at each level of risk.

***Data Backup Plan***

Each functional area of PRO (Operations, Billing, Administration, etc.) will establish and implement a Data Backup Plan that ensures that each area of PRO will create and maintain retrievable exact copies of all PHI and other essential business information that is at a medium to high risk for destruction or disruption.

The Data Backup Plan must apply to all medium and high risk files, records, images, voice or video files that may contain PHI and other essential business information.

The Data Backup Plan must require that all media used for backing up PHI and other essential business information be stored in a physically secure environment such as a secure, off-site storage facility or cloud server. Where backup media remains on site, it will be kept in a physically secure location, different from the location of the computer systems have been backed up.

If an off-site storage facility or backup service is used, a written Business Associate Agreement must entered into with the outside party maintaining the data to ensure that the Business Associate will safeguard any PHI and other essential business information in an appropriate manner.

Data backup procedures and contingency plan shall be tested on a periodic basis to ensure that exact copies of PHI and other essential business information can be retrieved and made available whenever it is needed.

The HIPAA Compliance Officer will ensure that each functional area of the Company with medium and high risk to PHI has an appropriate Data Backup Plan in place.

***Disaster Recovery Plan***

To ensure that each functional area of PRO can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster affecting information systems containing PHI or other essential business information, each functional area will establish and implement a Disaster Recovery Plan.

The Plan must ensure that each area can restore or recover any loss of this information and the systems needed to make that information available in a timely manner.

The Disaster Recovery Plan will include procedures to restore PHI and other essential business information from data backups in the case of a disaster causing data loss.

The Disaster Recovery Plan will include procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.

The Disaster Recovery Plan must be documented and easily available to the necessary personnel at all time, who should be trained to implement the Disaster Recovery Plan.

The disaster recovery procedures outlined in the Disaster Recovery Plan must be tested on a periodic basis to ensure that PHI and other essential business information and the systems needed to make e-PHI available can be fully restored or recovered.

The HIPAA Compliance Officer will ensure that each functional area of the Company with medium and high risk to PHI has an appropriate Disaster Recovery Plan in place.

***Emergency Mode Operation Plan***

Each functional area of PRO must establish and implement (as needed) procedures to enable continuation of administrative, patient care, and billing and business processes for protection of the security of PHI and other essential business information while operating in emergency mode.

Emergency mode operation procedures outlined in the Emergency Mode Operation Plan must be tested periodically to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.

The HIPAA Compliance Officer will ensure that each functional area of the Company with medium and high risk to PHI has an appropriate Emergency Mode Operation Plan in place.

# Pro Policy 1200.26

## Policy 26: Policy on Disaster Management and Recovery of e-PHI

### Purpose

PRO is responsible under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") for ensuring that we have a process in place to ensure that we can recover from the catastrophic disruption of our information system and loss of any data or information, especially electronic protected health information (" e-PHI"), which may be stored on that system. This policy will be followed in an emergency situation such as or disaster such as fire, vandalism, terrorism, system failure, or natural disaster.

### Scope

This policy applies to all PRO staff members who create, receive or use PHI and e-PHI, and any other confidential patient or business information. It is intended to cover all information system hardware, software and operational procedures. The HIPAA Compliance Officer shall be the primary party in charge of disaster management and recovery.

### Procedure

To ensure that PRO will be able to recover from a serious information system disruption, including situations that could lead to the loss of data in the event of an emergency or disaster (such as fire, vandalism, terrorism, system failure, or natural disaster) the following procedures are established:

1. A disaster recovery plan will be established and implemented to restore or recover any loss of e-PHI and any loss or disruption to the systems required to make e-PHI available.

1. The disaster recovery plan will be developed by staff members responsible for the maintenance of the security and integrity of the information system and will be reviewed and approved by the HIPAA Compliance Officer and senior management.

1. The disaster recovery plan must include:

1. A data backup plan including the storage location of backup media.

1. Procedures to restore e-PHI from data backups in the case of an emergency or disaster that results in a loss of critical data.

1. Procedures to ensure the continuation of business critical functions and processes for the protection of e-PHI during emergency or disaster situations.

1. Procedures to periodically test data backup and disaster recovery plans.

1. Procedures to periodically perform an application and data criticality analysis establishing the specific applications and e-PHI that is necessary to maintain operation in an emergency mode.

1. Procedures to log system outages, failures, and data loss to critical systems.

1. Procedures to train the appropriate personnel to implement the disaster recovery plan.

1. The disaster recovery plan must be documented and easily available to the necessary personnel at all times.

# Pro Policy 1200.27

## Policy 27: Policy on Physical Security of PHI and e-PHI

### Purpose

PRO is obligated under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to establish physical safeguards to protect electronic protected health information ("e-PHI") and other PHI. This policy establishes our security measures to protect our electronic information systems, networks and applications and as well as buildings and equipment from natural and environmental hazards, and unauthorized intrusion.

### Scope

This policy applies to all PRO staff members. All staff members should be on the lookout for any potential problems that could jeopardize the security of electronically stored information, especially e-PHI. This policy describes our general approach to facility security and the steps necessary to prevent a breach in the physical security system in place. It also describes our general procedures to limit physical access to electronic information systems and the buildings and rooms in which they are housed, and our general procedures on disposal or reissuance of equipment containing e-PHI.

### Procedure

***Facility Access Controls***

Access to areas of our facility that contain our information system with e-PHI will be granted only to those with a verifiable and approved business need to have access.

All PRO staff members will be issued identification cards or badges for security purposes. These badges and identification must be displayed at all times while on the premises.

Access control will be established with physical hardware that prevents improper or inadvertent entry into a secure area. This hardware may include combination locks, swipe cards, smart cards and other devices on all doors housing our information system equipment.

Any space in a building that we share with another entity that contains PHI that we create, receive, maintain or transmit will be maintained at the same level of security as if we owned the space. Specifically, we will protect that area from access by others in the building who are not part of PRO.

Disabling or circumventing any of the physical security protections is strictly prohibited. Any problems with physical security measures must be reported to the HIPAA Compliance Officer immediately.

***Facility Security Plan***

The HIPAA Compliance Officer will be responsible for developing a facility security plan that protects our buildings from unauthorized physical access, tampering, and theft.

The plan will incorporate hardware to limit access to our buildings to only those persons with proper keys and/or access codes.

PRO will maintain a current list of all staff members who have authorization to access our facilities with PHI. Where appropriate, PRO will install security systems including video surveillance to protect PHI and to ensure the security of our information systems.

***Access Control and Validation Procedures***

PRO has established procedures for controlling and validating a staff member's access to our facilities. Access to various areas of the facilities will be based on the role of the staff person and their need to access a particular area.

Access to locations that house our systems, networks or applications with PHI that we create, receive, maintain or transmit will have the greatest limitations on access, and access to these critical areas will be reviewed frequently by management and the HIPAA Compliance Officer.

***Maintenance Records***

To help ensure that our physical security systems are in continuous operation, PRO has developed a maintenance program for all security devices, including locks, keypads, and other access devices.

Any repairs or change outs of any security devices will be recorded.

***Workstation Security and Use***

A "workstation" is defined as any electronic computing device, such as a desktop computer, laptop computer, mobile electronic device or any other device that is used to create, receive, maintain or transmit PHI.

All workstations (including fixed locations such as in our billing or business office and mobile workstations such as with portable electronic devices for field use) should be password protected so that they may not be accessed without authentication by an authorized user.

All workstations are set up to lock out after a set time period so that if the staff member is no longer using the workstation for a set period of time, access will not be permitted without the proper password.

Procedures are established for each work area, depending on the nature of the work area to limit viewing of workstation device screens to only those operating the workstation wherever possible.

1. In office areas, all screens should be pointed away from hallways and open areas. The screens should be pointed away from chairs or other locations where non staff members, such as patients, may be.

1. In field operations, ambulance personnel will need to follow procedures to ensure that the devices are not left in an open area, such as a countertop in the Emergency Department.

Workstations will be set so that staff members may not inadvertently change or disable security settings, or access areas of the information system they are not authorized to access.

Only those authorized to access and use the workstation will be permitted to use the workstation.

No software may be downloaded or installed on the workstation in any manner without prior authorization. (This prohibition includes computer games, screen savers, and anti-virus or anti-spam programs).

All staff members will log out or lock workstations whenever they are left unattended or will not be in use for an extended period of time.

All portable workstation devices will be physically secured wherever possible when not in use. Laptops will be locked with security cables and other mobile devices will be locked physical locations or in an appropriate storage compartment when not in use.

Remote access to access e-PHI on our information system must be approved by PRO.

***Disposal of Hardware and Electronic Media Devices and Media Controls***

PRO carefully monitors and regulates the receipt and removal of hardware and electronic media that contain PHI and other patient and business information into and out of our stations and other facilities.

As a general rule, simple deletion of files or folders is not sufficient to ensure removal of the file or data. This simply removes the directional "pointers" that allow a user to find the file or folder more readily. Deleted files are usually completely retrievable with special software and computer system expertise.

PRO has in place the following procedures governing the disposal of hardware, electronic media, and e-PHI stored on hardware and other electronic media:

- Sanitizing Hard Disk Drives. All hard disk drives that have been approved by the HIPAA Compliance Officer for removal and disposal (or taken out of active use) shall be sanitized so that all programs and data have been removed from the drive. PRO will follow industry best practices (such as the U.S. Department of Defense clearing and sanitizing standard – DoD 5220.22-M) when cleaning off hard drives.

Proper sanitizing usually involves a reformatting of the hard drive in a secure manner with an approved wipeout utility program. Degaussing software may need to be used to ensure total removal of files.

No hard drive will be reissued, sold or otherwise discarded until the drive has been sanitized.

- Media Re-Use. All e-PHI and other patient and business information shall be removed from any media devices before they are made available for reuse.

- Accountability. PRO tracks the movement of all computer hardware, workstations, and data storage devices. Movement both within the organization and outside the organization is tracked.

- Data Backup and Storage. Each information system area will create an exact copy of all e-PHI when necessary immediately prior to any movement or disposal. This procedure is in addition to the standard routine backup protocol to ensure that all e-PHI is preserved before potential compromise.

- Destruction of Paper and electronic PHI. When destroying and/or permanently removing PHI from electronic media for any purpose, PRO shall adhere to HHS's "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals." In accordance with that Guidance, paper, film, or other hard copy media shall be shredded or destroyed such that the PHI cannot be read or otherwise reconstructed. Electronic PHI is considered to be destroyed or permanently removed from electronic media when the media that contain the PHI have been cleared, purged, or destroyed consistent with "NIST Special Publication 800–88, *Guidelines for Media Sanitization*," such that the electronic PHI cannot be retrieved. (NIST Special Publication available at: nist.gov).

# Pro Policy 1200.28

## Policy 28: Policy on Electronic Information System Activity Review and Auditing

### Purpose

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires PRO to monitor and audit its electronic information system used to create, receive, maintain or transmit electronic protected health information ("e-PHI") so that quality assurance procedures will detect and address problems with the system. PRO needs to identify the specific actions that have taken place such as timing and completion of back-up procedures, tracking server file access, and tracking power interruptions and other unusual events that could compromise our system and threaten the integrity of e-PHI.

### Scope

This policy applies to all PRO staff members who are responsible for monitoring and maintaining our electronic information system or are responsible for its security. The policy also applies to staff members assisting with the audit and review process. The HIPAA Compliance Officer shall have overall responsibility for monitoring, maintaining, and overseeing the security of our electronic information system and conducting audits.

### Procedure

The HIPAA Compliance Officer will develop procedures to document the creation, receipt, maintenance and transmission of e-PHI within the information system.

The HIPAA Compliance Officer will review the records of information system activities, including a review of audit logs, security incident tracking reports, back-up records, etc., as necessary.

Uses and disclosures need not be documented for purposes of an audit trail if the use is made entirely within the internal information system and the use did not involve any outside parties.

Disclosures that are required to be accounted for under HIPAA shall be recorded and tracked. Generally all non-patient authorized disclosures that are not related to treatment, payment and healthcare operations will be accounted for. An accounting of these disclosures must include:

1. The date of the disclosure;

1. The name and address of the organization or person receiving the disclosure (if known);

1. A brief description of the PHI disclosed; and

1. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.

# Pro Policy 1200.29

## Policy 29: Policy on Third Party Access to e-PHI

### Purpose

PRO is required by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to control access to our physical locations, such as stations, buildings, garages and offices, vehicles, and secured areas where our electronic protected health information ("e-PHI") is stored as well as system hardware, software, or other mobile electronic devices that are used to create, receive, maintain or transmit e-PHI. This policy outlines our approach to limiting third party access to our e-PHI while at the same time, permitting authorized access in the event that our contingency plan is operation.

## Scope

This policy applies to all PRO staff members who control third party access to our e-PHI and systems, hardware and mobile electronic devices used to create, receive, maintain or transmit e-PHI. It is intended to cover all physical locations that house our information system hardware, software and related devices and equipment that are utilized to create, receive, maintain or transmit e-PHI at PRO.

## Procedure

### *Access During Contingency Operations*

The HIPAA Compliance Officer will work with individuals who manage electronic information systems to determine contingency plans and procedures that should be implemented in the event of the need to restore lost data and to maintain uninterrupted access to e-PHI.

The HIPAA Compliance Officer will identify outside parties who have permission to access our electronic systems and secured areas in the event that restoration and preservation of data is necessary.

The HIPAA Compliance Officer will work with management to develop a "call list" of persons who need immediate notification when the contingency plan is in operation.

### *Facility Security*

The HIPAA Compliance Officer will work with management to determine what outside parties, in general, should have access to e-PHI and the electronic information system and determine the extent of that access.

The HIPAA Compliance Officer will maintain an inventory of all software, hardware and mobile electronic devices used to create, receive, maintain or transmit e-PHI at PRO. That inventory should include:

1. A unique identification number for hardware and other devices that are part of the electronic information system.

1. A file to catalog all software, hardware and mobile electronic devices with their unique identification numbers.

Any discrepancies in the current inventory of software, hardware and mobile electronic devices will be reported to management and will be investigated to ensure that there is a proper accounting of all items and to determine whether further action may need to be taken in response to the loss of an item (*e.g.*, breach notification in the event of a breach of unsecured PHI.

If PRO implements keypad access to physical facilities, the HIPAA Compliance Officer will ensure that access codes are changed or disabled when staff members leave.

There will be measures at the entrance to PRO's facility and at key access points that require personal identification, so that only authorized parties gain access to areas where e-PHI can be accessed. These procedures will be reviewed periodically to ensure only authorized persons with a legitimate purpose for access actually have access to the facility or secured area.

***Access Control and Validation***

The HIPAA Compliance Officer will maintain a list of all third parties with approved access to e-PHI and the electronic information system. This list will include names of approved vendors and other outside parties who have permission to access our facilities and secure areas.

Software testing and other maintenance or service of the electronic information system will be carefully monitored by the HIPAA Compliance Officer to ensure that only necessary e-PHI is accessed and that e-PHI is not being improperly used or disclosed.

PRO will ensure that only approved parties with a legitimate need to access our electronic information system are granted access. If outside parties need physical access to an area with e-PHI, they must present valid credentials (such as a driver's license and business card or badge).

***Maintenance Records***

The HIPAA Compliance Officer will ensure that all repairs and maintenance to the electronic information system hardware, software and mobile electronic devices is properly logged and documented.

The repair or maintenance records will contain, at a minimum:

1. Name of person completing the maintenance or repair;

1. Purpose of the maintenance or repair;

1. Name of person at PRO authorizing the maintenance or repair;

1. Date and time the work started and ended; and

1. Brief description of the work completed and the outcome of it (more work required, alternative procedure to put in place, etc.)

The HIPAA Compliance Officer will periodically review the documentation of maintenance and repairs to determine trends or changes in procedures to e-PHI security that should be made.

***Accountability***

PRO shall have a way to record the addition or removal of any hardware, software or mobile electronic devices to or from our electronic information system.

No hardware, software or mobile electronic devices will be added to the electronic information system without notifying the HIPAA Compliance Officer. The HIPAA Compliance Officer shall review any additions and ensure that any addition will comply with PRO's HIPAA Policies and Procedures.

To maintain security and to help prevent viruses from attacking our information system, no downloads or software additions are permitted without approval of management and only after consultation with the HIPAA Compliance Officer.

# Pro Policy 1200.30

## Policy 30: Policy on Creating Backups of e-PHI

### Purpose

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires PRO to back up and preserve all e-PHI created, received, used, and stored by PRO in the event of an emergency or disaster. This policy outlines the procedures for preserving and protecting e-PHI and other important business information from tampering, theft, fire, flood, and other physical damage. Key to this process is the proper replication of exact copies of data in a secondary system so that if the primary system fails, the data will be completely preserved and accessible.

### Scope

This policy applies to all e-PHI created, received, maintained or transmitted by PRO. Creating backups will be the responsibility of the manager in charge of the particular electronic equipment for his/her area of responsibility, in close coordination with the HIPAA Compliance Officer. This policy applies to all electronic equipment and devices that are used to create, receive, maintain or transmit e-PHI at PRO. This policy applies to all staff members and vendors or contracted parties who are responsible for completing backups of PRO's e-PHI.

### Procedure

***Physical Access Controls***

All backup systems will be located in a secure area, with limited access so that only those with responsibility for the backup system will have access to it.

Servers, backup drives and other data and information saving hardware will be located in a locked room.

Only authorized parties will have access to a physical location where backup devices are stored.

***Backup Schedule***

Data and information stored on any computers or electronic devices will, at a minimum, be backed up at sufficient intervals to ensure that critical data (especially PHI) can be restored and recovered immediately. A full system backup will be completed at least monthly.

PRO will verify that the backups are successfully completed at the end of each backup process to ensure that a complete replication of the data and information backed up has actually been created.

***Backup Schedule Logs***

The backup software will capture a list of all files and directories encountered and saved. Logs will be maintained and will contain information about successful backups, unsuccessful backups, backup media that was left in place and overwritten, when and where the media was sent or transmitted off-site, the success or failure of restore tests and bad media encountered which may affect our ability to obtain files from a previous backup.

A primary and secondary staff member will be assigned to rotate the media used for backups if PRO backs up e-PHI with physical media. This staff member will track the following information:

1. Whether the backup was successful;

1. Date and time the backup began and the date and time it was completed;

1. Description of any problems encountered during the backup; and

1. Verification that a check was made to ensure that the backup was complete.

***Marking and Storage of Backup Media***

All backup disks, drives, tapes or other physical backup media will be legibly and clearly marked that it is a backup, the date and time the backup was completed, and the initials of the staff member who completed the backup.

All backup tapes, drives and other physical storage media should be stored at a secure off-site location to ensure the preservation of all but the most recent data and information in the event of a catastrophic fire, flood, or other damage to the primary backup location. The media must be transported in a secure manner by a supervisor or other official. PRO may contract with a reputable vendor to manage its backup process and media storage. The vendor must execute a business associate agreement with PRO to ensure that the vendor will, among other things, protect the integrity of the data stored and protect it from improper use or disclosure. Security access controls implemented at the off-site backup and storage location must meet or exceed the security access controls of the source systems. In other words, information security at the backup storage location must equal or exceed the security where the primary computers and servers are located.

PRO may electronically backup PHI to a cloud server if PRO obtains a business associate agreement from the server agency and all PHI is maintained in a manner that enables PRO to meet is HIPAA compliance obligations.

***Data Retention***

Full system backups will be copied and/or archived.

Archived backups must be periodically tested to ensure that they are recoverable.

***Documentation***

The backup restore and recovery processes must be documented by the HIPAA Compliance Officer.

***Storage of Media Other Than Backups***

Old hard drives or other media storage devices that have been removed from the information system will be handled as follows:

1. If the device is to retain PHI, it will be stored in the same fashion as the backup devices.

2. If the device is to be taken out of service and no longer used to store PHI, it shall be “sanitized” and erased prior to disposal in accordance with PRO’s “Policy on Physical Security of PHI and e-PHI.”

***Emergency Contact information***

PRO will maintain a list of designated staff to be contacted in an emergency. A copy of this list will be kept in a secure location at the main facility and the off-site backup location (if applicable). The list must be kept up to date and readily accessible in case of an emergency. The list will also include vendor contact and support information and contacts for the off-site media storage location.

# Pro Policy 1200.31

## Policy 31: Policy on Encryption of e-PHI

### Purpose

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires PRO to consider encryption as a method for securing our electronic protected health information ("e-PHI") and to implement a mechanism to encrypt and decrypt e-PHI if PRO determines that doing so is reasonable and appropriate. Further, encrypting e-PHI consistent with the Department of Health and Human Services' ("HHS") "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals" will create the equivalent of a "safe harbor" for PRO in the event that there is a breach of PRO's PHI. It is the policy of PRO to use encryption consistent with HHS's Guidance wherever possible, as outlined in this policy.

### Scope

This policy applies to all PRO staff members who are responsible for the manner in which e-PHI is created, received, maintained or transmitted by PRO. The HIPAA Compliance Officer, in conjunction with appropriate information technology professionals, shall be responsible for implementing appropriate mechanisms to encrypt e-PHI consistent with this policy.

### Procedure

The HIPAA Compliance Officer shall, on a periodic basis, meet with appropriate parties, such as management, information technology professionals, software vendors, and others, to discuss the steps necessary to encrypt all e-PHI that PRO creates, receives, maintains or transmits consistent with HHS's Guidance at: http://www.hhs.gov/ocr/privacy.

The HIPAA Compliance Officer shall review or refer appropriate parties to the National Institute of Standards and Technology ("NIST") Special Publications referenced in this policy (available at: www.nist.gov) so that PRO implements appropriate technologies and methodologies to secure e-PHI as prescribed in the Publications.

The HIPAA Compliance Officer shall also annually review HHS's updated Guidance (available at: http://www.hhs.gov/ocr/privacy) for any additional resources referenced by HHS and ensure that those resources are furnished to appropriate parties.

Whenever possible, PRO shall convert all paper and hard copy PHI into electronic format and then secure it consistent with encryption methods outlined in this policy. Paper or other hard copy PHI should be scanned or otherwise converted into digital format and then the original hard copy should be shredded or destroyed in a manner that ensures that the PHI can no longer be read or otherwise reconstructed. If PRO utilizes an outside agency to shred, destroy or digitize paper and hard copy PHI, PRO shall enter into a business associate agreement with that outside party.

All e-PHI created, received, maintained or transmitted by PRO must be encrypted through the use of an algorithmic process that transforms data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. All encryption keys must be stored in a different

location than the data which it is meant to decrypt. PRO shall adhere to the following guidelines when encrypting PHI data in various forms:

1. PHI at Rest. For PHI data that is "at rest," (*i.e.,* PHI in databases, file systems, stored on flash drives, electronic device memory, and other structured storage methods), PRO shall utilize encryption processes that are consistent with NIST Special Publication 800-111, "*Guide to Storage Encryption Technologies for End User Devices*." (available at www.nist.gov)

2. PHI in Motion. For PHI data "in motion," (*i.e.,* PHI that is being transmitted through a network, wireless transmission, email, or other electronic transmission), PRO shall utilize encryption processes that comply with the requirements of Federal Information Processing Standards ("FIPS") 140–2. These include standards described in NIST Special Publications 800–52, "*Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*;" Special Publication 800–77, "*Guide to IPsec VPNs*;" or Special Publication 800–113, "*Guide to SSL VPNs*," and may include others which are FIPS 140–2 validated. (NIST Special Publications available at: www.nist.gov).

# Pro Policy 1200.32

## Policy 32: Policy on Security Incident Management

### Purpose

The Health Insurance Portability and Accountability Act ("HIPAA") requires PRO to track and appropriately respond to all incidents that could compromise our electronic protected health information ("e-PHI"). This policy establishes PRO's procedures for reporting a security incident and the steps that will be taken by PRO to investigate and take action when a potential or actual security incident occurs.

### Scope

This policy applies to all PRO staff members who utilize the electronic information system. Everyone at PRO is responsible to know what to do when confronted with a security incident. The Security/Breach Incident Reporting Form should be used in conjunction with this policy.

### Procedure

***Security Incident Defined***

A "security incident" is an attempted or successful unauthorized entry, breach or attack on the electronic information system that we use to create, receive, maintain or transmit e-PHI. Security incidents include unauthorized probing and browsing of the files, a disruption of service in our information system and incidents where e-PHI has been improperly altered or destroyed. Security incidents also include things such as a virus, hacking attempt or incident, "phishing" incident, malware installation, corrupt data or other similar incident involving PRO's information system.

***Reporting a Security Incident***

All staff members are responsible for immediately reporting a suspected security incident immediately to the HIPAA Compliance Officer or an immediate supervisor.

When a suspected security incident occurs, the HIPAA Compliance Officer shall have the reporting staff member and other members with knowledge of the incident complete PRO's "Internal Breach/Security Incident Reporting Form."

The HIPAA Compliance Officer will be responsible for initiating an immediate investigation to isolate the problem and take whatever action is necessary to protect the information system and e-PHI and other vital electronic information.

The HIPAA Compliance Officer will notify management immediately in the event the incident cannot be immediately corrected, or if any e-PHI or other vital information is altered or destroyed. Management will also be notified of any completed investigation and the outcome of the investigation.

In the event of unlawful activity via the use of PRO's information system, local, state, or federal law enforcement may be notified. That determination will be made by management with recommendation from the HIPAA Compliance Officer. The HIPAA Compliance Officer is responsible for coordinating communications with outside organizations and law enforcement.

Whenever a security incident is suspected or confirmed to have occurred, remedial action will be taken, including action against any individual staff members when it has been confirmed that they caused or contributed to the incident.

***HIPAA Compliance Officer Responsibility***

The HIPAA Compliance Officer is responsible for the following:

1. Initiating the appropriate incident management action, including restoration.

2. Determining the physical and electronic evidence to be gathered as part of the incident investigation.

3. Monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.

4. Determining if a widespread communication is required, the content of the communication, and how best to distribute the communication.

5. Communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.

6. Initiating, completing, and documenting the incident investigation.

7. Determining whether the incident may qualify as a breach of unsecured PHI requiring breach notification under PRO's "Policy on Breaches of Unsecured Protected Health Information."

# Pro Policy 1200.33

## Policy 33: Policy on Staff Member Electronic Communications

### Purpose:

PRO is required under the Health Information Portability and Accountability Act of 1996 ("HIPAA") to ensure that protected health information ("PHI") that we create, receive, maintain or transmit is not improperly disclosed through any means, including electronic means. The purpose of this policy is to prevent the improper use or disclosure of PHI through electronic means, while staff members are on and off-duty.

### Scope:

This policy covers any and all electronic communications of PRO staff members when those communications involve the use or disclosure of PHI created, received, maintained or transmitted by PRO. This policy applies to all staff members both on and off duty, whether using company or personal equipment.

### Procedure:

***General Rules Regarding Company Equipment***

All PHI created, received, maintained or transmitted using any "Company Equipment" is at all times the property of PRO and may be considered to be part of the official records of PRO. "Company Equipment" is any electronic device that is owned, leased, controlled, or used for the benefit of PRO. This includes, but is not limited to: computers, cell phones, cameras, USB drives, and other devices that are capable of creating, capturing, storing, and/or transmitting electronic information.

All Company Equipment shall remain at all times the property of PRO, even if being used for personal use.

PRO cannot guarantee the confidentiality of information stored on any Company Equipment, except that it will take all steps necessary to secure the privacy of all PHI in accordance with all applicable laws. Information stored on Company Equipment is subject to disclosure to law enforcement or other third parties at the sole discretion of PRO.

PRO may monitor activity on Company Equipment, our information systems and our network(s) at any time for the purpose of ensuring that PHI is not being improperly used or disclosed. This includes the ability to monitor internet activity and email, as permitted by law.

All internet activity (browsing, email, etc.) using Company Equipment must comport with PRO's HIPAA Policies and Procedures and staff members may not disclose PHI on the internet using Company Equipment unless the disclosure is authorized by PRO, would not violate HIPAA or other applicable federal and state laws, and the disclosure is for a legitimate, business-related purpose. For example, emailing demographic information about a patient to a patient's insurer for purposes of billing may be a permissible use.

***General Rules Regarding Personal Equipment***

Staff members must comply with PRO's HIPAA Policies and Procedures when engaging in internet activity on "Personal Equipment," both on and off-duty. "Personal Equipment" includes any internet-capable device that is not owned, leased or otherwise controlled or used for the benefit of PRO.

Where permitted by law to do so, PRO will investigate internet activity, whether on or off-duty, and take appropriate disciplinary action against staff members whenever PRO learns about a possible or actual violation of our HIPAA Policies and Procedures.

Staff members should consult with the HIPAA Compliance Officer whenever there is a question regarding whether an internet posting or internet activity might violate our HIPAA Policies and Procedures.

The following types of activities are prohibited at all times and can result in disciplinary action:

1. Posting, sharing, or otherwise disseminating any PHI relating to PRO patients without authorization from PRO.
2. Posting, sharing or otherwise disseminating information that could potentially identify a patient, including: photos, videos or other images of a scene or patient; a description of patient injuries, or; other scene activities that could be identified with a specific scene without authorization from PRO.

***Use of Company Electronic Mail***

PRO's email is intended to be used as a tool to facilitate communications on behalf of PRO.

All email transmissions that originate from PRO staff members on Company email must contain, at a minimum, a signature section that contains the following information:

1. The sender's full name;

1. PRO's name;

1. The telephone number of PRO; and

1. An approved notice and disclaimer.

Below the signature section, the following notice and disclaimer must appear on all transmissions from PRO staff members in at least 10 point font:

CONFIDENTIALITY NOTICE: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, and/or privileged information protected by law. If you are not the intended recipient, you may not use, copy, or distribute this e-mail message or its attachments. If you believe you have received this e-mail message in error, please contact the sender by reply e-mail and telephone immediately and destroy all copies of the original message.

***Facsimile Transmissions Using Company Fax Machine***

PRO's fax machine is intended to be used as a tool to facilitate communications and the exchange of information, including patient information that is needed to perform our services.

All outgoing facsimile transmissions using the Company fax machine must contain a cover sheet that includes at a minimum, the following information:

1. The name of PRO;
1. The name of the intended recipient;
1. The name of the sender;
1. Facsimile number of the recipient;
1. Telephone number of the sender;
1. Date of the transmission;
1. The number of pages in the transmission; and
1. An approved notice and disclaimer.

At the bottom of the facsimile cover sheet, the following notice and disclaimer must appear in at least 10 point font:

Confidentiality Notice: This facsimile transmission is confidential and is intended only for the review of the party to whom it is addressed. It may contain proprietary and/or privileged information protected by law. If you are not the intended recipient, you may not use, copy or distribute this facsimile message or its attachments. If you have received this transmission in error, please immediately telephone the sender above to arrange for its return.

***Images and Videos That May Contain PHI***

Staff members are strictly prohibited from capturing any images or videos that could potentially identify a patient PHI while on duty without the express permission of a supervisor. Staff members may carry a personal electronic device (such as a cell phone) that is capable of capturing images; but, staff members must adhere to our HIPAA Policies and Procedures when using the device and the device may never be used to capture PHI (unless expressly permitted by a supervisor). No other personal electronic devices that function as a camera and/or video recorder shall be carried by staff members while engaged in any work activities.

Staff members may only capture images or video while on-duty with a company-issued device and only for legitimate business-related purposes. Staff members must be authorized by PRO to capture images or video while on duty.

Images or videos taken with Company Equipment may only be disseminated in accordance with PRO's HIPAA Policies and Procedures and all such images and videos are the sole property of PRO.

Any images or videos that might identify a patient may not be posted on the internet without the express approval of PRO.

# Pro Policy 1200.34

## Policy 34: Policy on Staff Member Medical Records

### Purpose

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires PRO to treat protected health information ("PHI") contained in the medical records of our staff members with the same degree of protection as the PHI of our other patients. This policy provides guidance to management and staff concerning the privacy and security of PRO staff member medical records.

### Scope

This policy applies to PHI of all staff members and it applies equally to management and non-management staff members.

### Procedure

***Distinguishing PHI and Employment Records***

Health information that is obtained about staff members in the course of providing ambulance or other medical services directly to them is considered to be PHI under HIPAA.

Health information that PRO receives in its role as an employer is not considered to be PHI. Rather, the information is an employment record to which PRO does not have an obligation to extend HIPAA protections. For example, if a staff member submits a doctor's statement to a supervisor to document an absence or tardiness from work, PRO does not need to treat that statement as PHI. Other health information that could be treated as an employment record, and not PHI, includes:

1. Medical information that is needed for PRO to carry out its obligations under the FMLA, ADA and similar laws;

1. Information related to occupational injury, disability insurance eligibility, drug screening results, workplace medical surveillance, and fitness-for-duty-tests of employees.

***General Policy Regarding Staff Member's PHI***

1. PRO will, to the extent required by law, protect, use and disclose PHI it receives about staff members in accordance with HIPAA and our HIPAA Policies and Procedures.
2. Only those with a legitimate need to use or disclose PHI about staff members will have access to that information.
3. In accordance laws concerning disability discrimination, all medical records of staff will be kept in separate files apart from the employee's general employment file. These records will be secured, used and disclosed in accordance with applicable laws.

***General Policy Regarding Employment Records***

1. Employment records are <u>not</u> considered to be PHI. As such, PRO is not required to protect, use and disclose employment records in accordance with HIPAA.
2. Employment records that are not covered under HIPAA include, but are not limited to:

3. Information obtained to determine suitability to perform the job duties (such as physical examination reports);
4. Drug and alcohol tests obtained in the course of employment;
5. Doctor's excuses provided in accordance with the attendance policy;
6. Work-related injury and occupational exposure reports; and
7. Medical and laboratory reports related to such injuries or exposures, especially to the extent necessary to determine workers' compensation coverage.
8. Despite the fact that PRO is not required to protect, use and disclose employment records in accordance with HIPAA, PRO will limit the use and disclosure of these records to only those necessary to perform business-related functions authorized by law. PRO will also secure all employment records of staff members and ensure that only staff members with a legitimate need to have access to them, such as certain management staff, PRO's designated physician and state agencies pursuant to state law, have access to employment records.

# Pro Policy 1200.35

## Policy 35: Policy on Releasing PHI to Family Members and Others

### Purpose

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") permits PRO to release protected health information ("PHI") about patients to family members, friends and others involved in the treatment of the patient or payment for that treatment. This policy outlines our procedures for releasing PHI to family members and others involved in our patients' care.

### Scope

This policy applies to all PRO staff members who receive requests from family members, friends and others for PHI of patients of PRO. This policy does not apply to formal requests from patients or their personal representatives for: access to PHI; amendment of PHI; restriction of PHI; accounting of disclosures of PHI; or confidential communications. This policy shall apply to requests for PHI from family members of the patient or others who do not qualify as the patient's personal representative, but who are involved in the patient's care or payment for that care.

### Procedure

***General Procedure for Releasing PHI to Family Members and Others***

HIPAA permits PRO staff members to release PHI that is directly relevant to the patient's care or payment for care to family members, friends and others involved in a patient's care, or payment for that care, whenever releasing PHI to that individual would be in the best interest of a patient. PRO may also use or disclose PHI to notify family members or others about a patient's location, general condition, or death.

If an individual other than the patient or the patient's personal representative makes a request for PHI from a PRO staff member, the staff member shall first determine whether the patient about whom the request pertains to is present, competent and able to make healthcare decisions.

If the patient is present, competent and able to make healthcare decisions, the staff member should obtain the patient's agreement to share the requested PHI with the individual, or give the patient an opportunity to object. The staff member may ask the patient whether it is okay to talk to the individual and release PHI to them. Or, the staff member can simply infer from the circumstances that the patient does not object to sharing the information with the individual. For example, if the patient's neighbor asks to ride along in the ambulance and the patient smiles, the staff member could infer that the patient is fine with the neighbor riding along and overhearing any PHI that is discussed. Or, if the staff member starts asking the patient about his or her medical history and the patient motions for a family member to come over, the staff member can infer that the patient wants the staff member to speak with the family member about his or her medical history.

If the patient is unavailable or unable to make medical decisions because of a physical or mental reason at the time of the request, then the staff member may only disclose PHI to the requestor if the requestor is involved with the patient's treatment or payment for the patient's treatment and the staff member believes that releasing PHI to the requestor is in the best interests of the patient. First, the staff

member should ask the requestor what his or her relationship is to the patient. Then, the staff member should determine whether disclosure of PHI to the requestor would be in the best interest of the patient. In making this determination, the staff member should consider things such as:

1. Who the requestor is and what the requestor's relationship is to the patient

1. Whether the requestor appears to have a legitimate interest in the patient's care or payment for that care

1. Whether the staff member believes that the patient would want that requestor to know the PHI or whether the patient would benefit from the requestor knowing the PHI

If the patient is deceased, a staff member may release relevant PHI to family members and others who were involved in the deceased patient's care prior to death or payment for care, unless doing so would be inconsistent with any prior expressed preference of the patient. The staff member should only disclose PHI that is relevant to the requestor's involvement with the patient's care prior to death or payment for that care.