PHOENIX HOUSES OF FLORIDA Organizational Administration	Effective Date: 11/18 Last Revision: 04/20
Policy Name: Medical Records	Policy Number: 1D.5b

Policy

To ensure the confidentiality of Personal Health Information and compliance with current Health Insurance Portability and Accountability Act of 1996 "HIPAA" and 42 C.F.R. Part 2, it is our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements.

Federal confidentiality law and regulations (see 42 U.S.C. § 290dd-2, 42 C.F.R. Part 2) prohibit Phoenix Programs of Florida, Inc. and its personnel from complying with request or even acknowledging whether or not the person requester is seeking information on is or ever was a patient in a PH program. 45 CFR Parts 160-164.530(i); CFOP 50-2 must be adhered to as well.

Per 65D-30.0041(1)- Clinical records shall be kept secure from unauthorized access and maintained in accordance with 42 Code of Federal Regulations, Part 2, and subsection 397.501(7), F.S.

The release of information regarding this medical records policy is based on the following assumptions and MUST be sufficient:

- Phoenix Programs of Florida, Inc. has obtained written consent or an authorization or give the individual an opportunity to object to a use or disclosure, in order to use or disclose medical information.
- Any use or disclosure of confidential patient Protect Health Information carries with it the potential for an unauthorized use or disclosure that breaches confidentiality.
- These policies and practices shall be consistent with state and federal laws and regulations that have not been preempted by HIPAA & 42 C.F.R. Part 2. and its implementing regulations, including the privacy regulations that contain provisions relating to the release of information from patient records. The legal department and risk management are responsible for reviewing the laws and regulations specified to this policy and any new laws and regulations amending this policy to comply with changed provisions.

Procedure

All medical records request should be forwarded to the Medical Records Custodian of Florida immediately upon receiving request.

All persons authorized to release medical records and information must read, understand, and comply with this policy.

PHOENIX HOUSES OF FLORIDA Organizational Administration	Effective Date: 11/18 Last Revision: 04/20
Policy Name: Medical Records	Policy Number: 1D.5b

Phoenix Programs of Florida, Inc. will process requests for medical records in a timely and consistent manner providing sufficient consent s are in place.

Sufficient Consents should:
Include certain specific information in order to make consent sufficient:

- Name of Individual who PHI release may be disclosed- must name an individual, not an entity or organization
    - Also include address, phone number and Relationship/Title
- Specific purpose of the disclosure
- The type of information that may be released (all applicable boxes must be checked)
- Be current AND have an expiration date listed
- Minor must sign
- Notice Prohibiting Re-Disclosure

No employee shall release medical records without complying with this policy.

Phoenix Programs of Florida, Inc. must make all reasonable efforts not to use or disclose more than the minimum amount of PHI necessary to accomplish the intended purpose of the use or disclosure.

For all uses, disclosures, or requests to which the minimum necessary rule applies, Phoenix Programs of Florida, Inc. may not disclose and entire medical record, except in cases which the entire medical record is justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

In order for request to be sufficient, written authorization request must contain detailed, specific information directing the release of patient information. Authorizations must include the following information:

- Name and address of requesting individual
- Name of the patient
- Name of the person, including complete address, to whom the information is to be released
- Telephone number of individual requesting records and the relationship of that individual to the entity requesting records
- Purpose of the disclosure
- Information to be released
- Date signed and signature

PHOENIX HOUSES OF FLORIDA Organizational Administration	Effective Date: 11/18 Last Revision: 04/20
Policy Name: Medical Records	Policy Number: 1D.5b

Phoenix Programs of Florida, Inc. shall maintain these record management procedures regarding content, organization, access, and use of records.

The record management system shall meet the following additional requirements per 65D-30.0041(1) (a) (b) (c) (d) (e):

- Original clinical records shall be signed in ink and by hand or electronically.
- Record entries shall be legible.
- In instances where records are maintained electronically, a staff identifier code will be accepted in lieu of a signature.
- Documentation within records shall not be deleted; and
- Amendments or marked-through changes shall be initialed and dated by the individual making such changes.

Prohibition of Re-disclosure

Each disclosure outside the practice will contain the **Prohibition of Re-disclosure** notice form on top of all releases sent out.

This release states the following:

> The attached medical information pertaining to [name of patient] is confidential and legally privileged. Phoenix Programs of Florida has provided it to [name of recipient] as authorized by the patient. The recipient may not further disclose the information without the express written consent of the patient as authorized by law.
>
> This information has been disclosed to you from records protected by federal confidentiality rules (42 C.F.R. Part 2). The federal rules prohibit you from making any further discloser of information in this record that identifies a patient as having or having had a substance use disorder either directly, by reference to publicly available information or through verification of such identification by another person unless further discloser is expressly permitted by the written consent of the individual whose information is being disclosed or as otherwise permitted by 42 C.F.R. Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. (see 2.31) The federal rules restrict any use of the information to investigate or prosecute with regard to crime any patient with a substance use disorder, except as provided at 2.12©(5) and 2.65.

Revocation of Authorization

A patient may revoke an authorization by providing a written statement to the practice. The revocation shall become effective when the practice receives it.

Methodology for Disclosure Not Requiring Consent

Exceptions to disclosures with written consent requirement

• To medical personnel to the extent necessary to meet a bona fide medical emergency

• To qualified personnel for the purpose of conducting scientific research, management or financial audits, or program evaluation but individual patients cannot be identified by those personnel in any report or otherwise disclosed

• If authorized by a court order showing good cause (e.g., need to avert a substantial risk of death or serious bodily harm)

- Reports of child abuse and neglect. The restrictions on disclosure do not apply to the reporting under State law of incidents of suspected child abuse and neglect to the appropriate State or local authorities. However, Part 2 restrictions continue to apply to the original alcohol or drug abuse patient records maintained by the program including their disclosure and use for civil or criminal proceedings which may arise out of the report of suspected child abuse and neglect [42 CFR § 2.12(c)(6)]. Also, a court order under Part 2 may authorize disclosure of confidential communications made by a patient to a program in the course of diagnosis, treatment, or referral for treatment if, among other reasons, the disclosure is necessary to protect against an existing threat of life or of serious bodily injury, including circumstances which constitute suspected child abuse and neglect [42 CFR § 2.63(a)(1)].

Breach Notification Procedures:

Information obtained from: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

"Breach Notification Rule

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

Definition of Breach

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as

applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

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

Covered entities and business associates, where applicable, have discretion to provide the required breach notifications following an impermissible use or disclosure without performing a risk assessment to determine the probability that the protected health information has been compromised.

There are three exceptions to the definition of "breach." The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority. The second exception applies to the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

Unsecured Protected Health Information and Guidance

Covered entities and business associates must only provide the required notifications if the breach involved unsecured protected health information. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.

This guidance was first issued in April 2009 with a request for public comment. The guidance was reissued after consideration of public comment received and specifies encryption and destruction as the technologies and methodologies for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Additionally, the guidance also applies to unsecured personal health record identifiable health information under the FTC regulations. Covered entities and business associates, as well as entities regulated by the FTC regulations, that secure information as specified by the guidance are relieved from providing notifications following the breach of such information.

View the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

Breach Notification Requirements

Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In

addition, business associates must notify covered entities if a breach occurs at or by the business associate.

Individual Notice

Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or business associate, as applicable).

With respect to a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate. Covered entities and business associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual.

Media Notice

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

Notice to the Secretary

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual

basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

Notification by a Business Associate

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any other available information required to be provided by the covered entity in its notification to affected individuals.

Administrative Requirements and Burden of Proof

Covered entities and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach. Thus, with respect to an impermissible use or disclosure, a covered entity (or business associate) should maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required: (1) its risk assessment demonstrating a low probability that the protected health information has been compromised by the impermissible use or disclosure; or (2) the application of any other exceptions to the definition of "breach."

Covered entities are also required to comply with certain administrative requirements with respect to breach notification. For example, covered entities must have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures, and must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

Submit a Breach Notification to the Secretary

View Breaches Affecting 500 or More Individuals

Breaches of Unsecured Protected Health Information affecting 500 or more individuals

- Per 42 CFR pt.2 Breach Instructions:
    - **§ 2.22 Notice to patients of federal confidentiality requirements.**
        - **(a)** *Notice required.* At the time of admission to a part 2 program or, in the case that a patient does not have capacity upon admission to understand his or her medical status, as soon thereafter as the patient attains such capacity, each part 2 program shall:
        - **(1)** Communicate to the patient that federal law and regulations protect the confidentiality of substance use disorder patient records; and
        - **(2)** Give to the patient a summary in writing of the federal law and regulations.

- **(b)** *Required elements of written summary.* The written summary of the federal law and regulations must include:
- **(1)** A general description of the limited circumstances under which a part 2 program may acknowledge that an individual is present or disclose outside the part 2 program information identifying a patient as having or having had a substance use disorder;
- **(2)** A statement that violation of the federal law and regulations by a part 2 program is a crime and that suspected violations may be reported to appropriate authorities consistent with § 2.4, along with contact information;
- **(3)** A statement that information related to a patient's commission of a crime on the premises of the part 2 program or against personnel of the part 2 program is not protected;
- **(4)** A statement that reports of suspected child abuse and neglect made under state law to appropriate state or local authorities are not protected; and
- **(5)** A citation to the federal law and regulations.
- **(c)** *Program options.* The part 2 program must devise a notice to comply with the requirement to provide the patient with a summary in writing of the federal law and regulations. In this written summary, the part 2 program also may include information concerning state law and any of the part 2 program's policies that are not inconsistent with state and federal law on the subject of confidentiality of substance use disorder patient records.

Penalty & Violations

All supervisors are responsible for enforcing the policy. Employees who violate this policy are subject to discipline up to and including termination from employment in accordance with Phoenix Programs of Florida, Inc. Policy.

Fines for Violations can include:

- Potential criminal fines for violations of 42 C.F.R. Part 2 (up to $5,000).
- Potential civil fines for violations of HIPAA (up to $1.5 million per calendar year for all violations of identical provision).

Patient Education

To facilitate the timely and proper release of information, the practice will provide patients an explanation of the release of information as part of the admission process.