Policy and Procedures Manual
Authority: Medical Director

Policy #: 7-010D

Effective Date: 7/29/01

Revision Date(s): 5/07/04, 06/23/14, 7/24/2020

Subject: **Confidentiality/General Policy on Confidentiality of Resident Identity and Records**

Policy:
Drug and Alcohol Treatment Programs demonstrate adherence to federal and state confidentiality laws and regulations with regard to resident identity, resident records, and staff access to resident records. Confidentiality of resident identity and resident records is maintained for every resident and every resident record in accordance to applicable federal and state laws and regulations, including but not limited to 42 CFR Part 2 (regarding Confidentiality of Alcohol and Drug Abuse Patient Records) and 45 CFR Part 164, Subpart E (regarding Privacy and Individually Identifiable Health Information) known as HIPPA.

Applicable procedures have been developed to protect the agency and affiliated organizations from liability and to protect the resident from the possibility of exposure to stigma.

This general policy on confidentiality covers the organization's policies and procedures regarding: Staff Access to Records; Confidentiality/Resident Access to Records; Security of Resident's Records; Informed and Voluntary Consent and Release of Information without Resident Consent. If any of these sections contradict another, the section that is more protective of resident confidentiality shall apply.

Scope:
This general policy on confidentiality is applicable to all staff that comes into contact with information about individuals receiving, having received, or having applied to receive substance abuse treatment.

It also applies to the following individuals:

- Holder: an individual or program in possession of such information may not release it except as authorized by the patient or as otherwise permitted by the regulations.
- Seeker: anyone seeing information may not compel its disclosure except as permitted by the regulations.
- Receiver: anyone who receives such information may not **redisclose** it without patient consent or as otherwise authorized by the regulations.

Procedure:

A. Confidentiality Generally

1. Records and any other information (recorded or not) of the identity, diagnosis, prognosis, or treatment of any resident will be confidential and may be disclosed only as expressly permitted pursuant to this Policy. For the purposes of this policy, to disclose shall mean: to communicate any information, including all protected health information as that term is defined within HIPAA, that would identify any resident or any person who has sought and/or received treatment at a Firetree facility, either directly, by reference to publicly available information, or through verification of such identification by another person.

2. Firetree will keep and maintain a written record of all resident-oriented information and data that is disclosed.

3. Staff are expected to strictly adhere to all confidentiality requirements. A breach of confidentiality is considered a serious violation of policy. Written reprimands, suspensions without pay, demotion, and termination are forms of disciplinary actions that the governing body implements for employee infractions

that are considered a serious detriment to operations or are repetitive. Employee disciplinary actions are made part of the staff's personnel record and include a written narrative of the specific violation, disposition imposed, effective date of the discipline, any appeal actions, and progressive consequences for reoccurrence.

4. In the event of an impermissible disclosure of protected information Firetree shall notify the individuals whose information was or was reasonably believed to have been breached. The notifications shall include the following:

   a. A brief description of what happened including dates of the breach and the discovery;

   b. A description of the types of information that was involved in the breach;

   c. The steps that the individuals should take to protect themselves from harm due to the breach

   d. A brief description of what Firetree is doing to investigate the breach and to mitigate the loss and harm to individuals

   e. Contact procedures for individuals to ask questions

B. Consent

1. Programs require voluntary consent authorizing the release of information from a resident prior to the disclosure of any verbal and or written protected health information. This consent shall be in writing and shall include each of the following elements:

   a. The name of the program or facility disclosing the information.

   b. The name of the specific person or agency that is to receive the information.

   c. The name of the resident who is the subject of the disclosure.

   d. The purpose of or need for the disclosure.

   e. How much and what type of specific information will be disclosed (the disclosure must be limited to the information which is necessary to carry out the stated purpose).

   f. A statement allowing for the revocation except to the extent that the program has already acted in reliance on it.

   g. The dates time or condition of expiration, which will last no longer than reasonably necessary to serve the purpose for which it was given.

   h. Signature of client and/or other authorized person and date.

   i. Signature of witness and date.

   j. Copy to client as either being accepted or declined.

   k. Accompanying notice of prohibition of redisclosure.

2. Any staff member who is involved in the release of information concerning a past or present resident to any individual, agency, or institution obtains a written Consent for Release of Confidential Information from that resident prior to the release of information.

3. Staff members complete the approved standardized form for the Release of Client Information.

4. The staff member completing the document ensures that the release of information form is filled out correctly and that all requirements of the consent are made clear to the client.

5. The client acknowledges acceptance or refusal of a copy of the consent in the area identified on the Release of Information document.

6. The staff member obtains a signature of the client or person authorized to act in the behalf of the client, and a witness along with the date upon which each party signed the document.

7. Upon receiving the dated signatures of the client and a witness, the original consent form becomes a part of the client file.

8. A copy of the prohibition of re-disclosure statement accompanies all information being released.

9. The original signed and dated authorization for release of information is filed as a permanent part of the client file.

10. Upon receiving a written or verbal request to revoke the consent for disclosure of client information the staff member notifies the primary counselor who takes the following course of action:

    a. The counselor makes a written notation regarding the revocation, sign and date on the original consent to release form and;

    b. Make an entry in the Individual Progress notes documenting the client revocation of consent to release information.

11. No further information is released to the individual or agency named on the revoked client consent form unless another appropriately completed form has been signed permitting release of information.

12. Upon entering the program the intake worker will obtain a release of confidential information for the organization. This release will be for the purpose of allowing internal communication between facilities. Internal communication between facilities is important for supervision, consultative, and administrative purposes.

13. Translation for Spanish speaking clients will be provided and reasonable accommodations will be provided for other languages.

C. Without Consent

1. Internal Program Communications - Staff will attempt to secure a specific release of information that allows for the disclosure of information to the corporate office of Firetree, Ltd. for the purpose of central billing or record keeping. In situations where the client refuses to permit disclosure of information required by the agency for billing purposes the refusal shall be documented in the client file. The completed release of information form shall be maintained in the client file.

2. Communications that do not Disclose Patient-Identifying Information - Staff who uses a client for the purpose of a case study shall review the case with the Clinical Director during clinical supervision. The purpose of this review will be to ensure that information being utilized in the case study does not disclose patient identifying information or that the information does not reveal the program name. Under no circumstances shall this section allow the disclosure, without consent, of a resident's protected health information, as that term is defined in HIPAA.

3. Medical Emergency. Covered Programs may Disclose Covered Information to medical personnel to the extent necessary to meet a bona fide medical emergency in which the patient's prior informed consent cannot be obtained. Immediately following Disclosure, the Disclosure must be documented in writing in the patient's records, setting forth

a. the name of the medical personnel to whom Disclosure was made and their affiliation with any health care facility

b. the name of the individual making the Disclosure

c. the date and time of Disclosure, and

d. the nature of the emergency.

4. Crime on Premises/Against Personnel. In the event of a crime or a threat to commit a crime on the premises of a Company Affiliate or its respective departments, or against personnel of the Covered Program, Disclosure of Covered Information to law enforcement is permitted to the extent the information:

a. is directly related to a patient's commission of a crime on the premises of the Covered Program or against personnel of the Covered Program or to a threat to commit such a crime; and
b. is limited to the circumstances of the incident, including the patient status of the individual committing or threatening to commit the crime, that individual's name and address, and that individual's last known whereabouts. The Privacy Official shall be consulted prior to any Disclosure of information pursuant to this provision.

5. Child Abuse. Firetree may report incidents of suspected child abuse and neglect as required by and in accordance with state law. However, the restrictions under 42 CFR Part 2 continue to apply to the original resident records including their Disclosure and use for civil or criminal proceedings which may arise out of the report of suspected child abuse and neglect. Accordingly, if, after a report is filed with relevant Information, a subpoena for Information is subsequently issued in connection with civil or criminal proceedings which arise from the report of suspected child abuse and neglect, the subpoena should be addressed in accordance with the other relevant sections of this Policy. The General Counsel shall be consulted prior to any Disclosure of information pursuant to this provision. Questions regarding state law and the extent of Covered Information subject to Disclosure under state law relating to suspected child abuse and neglect shall be referred to the General Counsel.

6. Audits: The following entities may review confidential information during the course of an audit without resident consent: 1) A government agency that funds or regulates a facility; or 2) any entity that provides financial assistance or any third-party payer covering residents in a facility.

a. In all cases de-identified information will be used in the course of the audit

b. If it is not feasible to use de-identified information then resident-identifying information may be used and viewed by the auditor(s)

c. Prior to review resident-identifying information the auditor(s) must agree in writing that they will comply with all relevant regulatory restrictions on use and re-disclosure of the identifying information and that the identifying information will only be used for the purpose of the audit.

d. When presented with a request by an auditor or peer review organization for a copy or removal of records the facility director will contact and consult with the Firetree General Counsel regarding the approval of the request.

e. Upon approval of the Firetree General Counsel, the Facility Director may allow for an auditor to copy or remove records.

f. Prior to releasing information the facility director must receive from the auditor a promise in writing to safeguard the confidentiality of the client, to re-disclose information only in accordance with the regulations and to destroy all patient-identifying information when the audit or evaluation is completed. The audit must have been initiated on site before the Facility Director will accept a written request to copy or remove records.

g. In responding to a subpoena no information should be released even if a judge signs the subpoena. The subpoena shall not be ignored. The person or program has a right to appear and object to the subpoena.

14. Upon receiving a subpoena the staff member will immediately contact the facility director. The facility director will notify and consult with the Firetree General Counsel, who, in consultation with management will determine the course of action. The staff member will follow the directions of the agency legal representative in responding to the subpoena.

15. When confronted with a search/arrest warrant staff will immediately contact the facility director or on-call administrator. The staff member will follow the directives of the Facility Director or on-call administrator.

16. Upon receiving notification of a search/arrest warrant the facility director or on-call administrator will produce a copy of regulations and explain that the program cannot cooperate with the warrant without a good cause court order.

17. In situations where the officers are attempting to serve the search/arrest warrant, the facility director will contact Firetree General Counsel and obtain a consultation on how to resolve the issue.

18. In a manner that does not reveal the identity of the client the Facility Director may in confidential manner and without disclosing that the client is in the facility have a staff member contact the client. The staff member will notify the client of the presence of the law enforcement officer and the purpose of the search/arrest warrant. The client will be afforded the opportunity to voluntarily surrender himself or herself to the legal officer.

19. In situations where the client is unwilling to surrender himself or herself to the legal officer the facility shall continue to protect the confidentiality of the client.

20. If the officer insists on entry staff members will not forcibly resist but will complete a facility incident report documenting the attempt to protect client confidentiality.

21. The Facility Director will inform the client, as readily as possible, that the information has been disclosed, to whom it was disclosed and for what purpose it was disclosed. This notification shall be documented in the client file and must reflect the following information:

    a. the name and affiliation of the recipient of the information

    b. the name of the individual making the disclosure

    c. the date of the disclosure

    d. the nature of the disclosure

22. Staff are advised to consult with immediate supervisors, clinical directors, facility directors, the corporate clinical director and the legal representative of Firetree, Ltd. when there are questions regarding the appropriate release of information without client consent.

D. Security of Client Records

1. Paper Files

    a. All client files are secured in a locked filing cabinet that is located in a locked storage area.

    Case File Security

    1. The file cabinet containing case files shall be marked "Confidential."
    2. Individual case files shall be marked "confidential."

3. Major pieces of information placed in case files shall be marked "confidential"
4. The file cabinet containing case files shall be secured at all times.
5. Case files shall be tracked via a sign-out sheet and replaced immediately after staff has completed work.
6. Case files shall not be removed from the facility premises.

b. Staff members authorized to have key access to the client alcohol and drug treatment files are the Facility Director, Clinical Director/Lead Counselor, Assistant Director, Addiction Counselor, Administrative Assistant, Compliance Officer and other members of the Quality Assurance team and the Licensed Medical Staff.

2. Electronic Files

The Enterprise Manager system has security and confidentiality embedded within the system. All active employees receive a user name and password. The passwords are changed quarterly or when it is determined to be needed. A role is assigned to each employee based on the HIPAA principle of minimum necessary to do their job. The main roles that are in the EM system are program monitor, case manager/counselor, case manager supervisor, facility director, fiscal, and medical. Program monitor role allows the client to access only information pertinent to their job client information folder, medical (modified), admission/intake. Case Manager/counselor role includes the program monitor rights as well as access to their own client case files that their supervisor has granted them rights to access. They have a modified medical folder allowing them to know the basics such as allergies, dietary modification, and medications. Case manager supervisor includes case manager/counselor rights to all client case files as well as the access to assign clients to counselors. Clinical director provides facility wide access for case management but does not grant fiscal or medical access. Director has the broadest rights to run the facility including HR. They can add clients and employees. Fiscal has program monitor rights and rights to the fiscal module for client trust fund accounting and billing.

Medical has program monitor rights and medical rights to the medical folders of each client. Auditor roles have read only access and may be designated for certain sections of the system.

All access is tracked. No entry in Enterprise Manager is deleted; it is voided/strike thorough. EM has a separate tracking database that tracks all entries and changes in the system. It tracks all content and what user perform the transaction.

3. Approval for access to files

Access to case files is only authorized to staff as follows:

a. Access is related explicitly to the fulfillment of specific job functions

b. All requests for case file information from any source shall be made in writing to the Facility Director

c. Oral discussion of the content of the case file is prohibited except for information disseminated to program staff during case review. Information is limited to a "need to know" basis and is limited to that information necessary to set and review program plan goals and the assessment of the individual's adjustment to the program.

Standard: 709.28(a)
Cross-Reference to Standard:
ACA: 4-ACRS-4C-19, 4-ACRS-6A-04

PA Depart of Health: Confidentiality/ Staff Access to Records 709.28 (a)(2); Confidentiality/ HIV Related Information; Confidentiality/ Client Access to Records 709.30 (3); Confidentiality/ Security of Client's Records 709.28 (b); Confidentiality/ Informed and Voluntary Consent 709.28 (c) (1,2,3,4,5,6), 709.28 (d); Confidentiality/ Release of Information without Client Consent 709.28(e)(1,2); and Confidentiality/ Reporting Suspected Child Abuse 709.28 (e)(2)
CARF 1.E.2
DPW: None
Cross-referenced Policy: #7-020, #10-050, #10-051, #6-080, #7-021D
Superseded Standard: (ACA 3-ACRS-1C-17, 1E-06 to 1E-08, 4E-24), RI.1, RI.1.5, RI.1.5, RI.2.2, IM.2, IM.7.2.10, RI.1.2.2, DPW: 5100.55, HIPAA 1996, Public Law 104 - 191
Supporting Documentation: consent forms, Consent to Obtain Confidential Information
Related Forms: Resident Contract & Consent to Participate (form # 20), Orientation and Consent to Treatment (form # 73), medical consent forms, Consent to Release (form #32)