RAVENWOOD HEALTH

SUBJECT: Client Confidentiality and Record Security | **POLICY AND PROCEDURE: #803**

EFFECTIVE DATE: 09/23/2003 | **REVIEW DATE: 10/27/2026**
BOARD APPROVAL: 9/24/2009 | **Next Review Date: 10/27/2028**

Policy:
Ravenwood Health (the "Agency") staff and/or individuals acting within Ravenwood Health shall manage Protected Health Information (PHI), confidential information, clinical data and the clinical record in a manner that preserves the privacy and confidentiality of clients of the Agency, in compliance with the Health Insurance Portability and Accountability Act (HIPAA), 42 C.F.R. Part 2, and applicable state law.

Definitions:
Privacy - an individual's right to control the access to, use, and disclosure of their personal health information.
Confidentiality – the safekeeping of data/information so as to restrict access to individuals who have need, reason or permission for such access.
Data Integrity – the protection of data from accidental or unauthorized intentional change.
Blackbox – limiting or restricting someone's access to a chart in carelogic.

Procedure:
Upon the hiring or inclusion of staff, volunteers, interns and/or agents to the agency, they will be informed and/or oriented to the client confidentiality and record security policy and procedure. Should this policy and procedure undergo changes or updates, they will be communicated to all staff, volunteers, interns and/or agents of the agency.

A. Confidentiality of the Clinical Record
1. Agency staff shall comply with the following:
- Handle personal health information, clinical data and the clinical record in a manner that maintains Data Integrity and a client's privacy and confidentiality in accordance with professional ethics, accreditation standards and legal requirements:
    a. Staff will collect and use only the minimum necessary client information for the purpose of providing services and supporting the delivery, payment and quality of those services.
    b. Staff will not use client information for non-health-care purposes, such as direct marketing, employment or credit evaluation purposes.
- Refrain from conveying to anyone outside of the Agency that a client attends or receives services from the Agency, or disclose any information identifying a client as a client, unless the client consents in writing for the release of information, or the disclosure is made to: (i) medical personnel for purposes of treating a bona fide medical emergency; or (ii) qualified service organization personnel for research, audit, or program evaluation purposes in accordance with 42 C.F.R. Part 2 (See Release of Information Policy and Procedure). If a client has been court ordered to treatment, the Agency may disclose only the information specified in the court order, which may include dates/times of
scheduled appointments, attendance or non-attendance in treatment, and appointment status (e.g. appointments were cancelled, or client did not show) without a written

Release of Information, provided the disclosure does not exceed the scope of the court order;

- Remove personal identifiers to the extent possible for uses and disclosures of clinical information, consistent with maintaining the usefulness of the information;
- Utilize protected clinical information for the purpose identified or as required by law or regulation and not further disclose without client authorization (See Release of Information Policy and Procedure);
- Use secure password(s) while documenting clinical information in client's EHR (electronic health record). Passwords will not be shared with others. Computer work stations shall be locked when not in use.
- Use a code with electronic signatures consisting of a combination of letters, numbers, characters, or symbols that are adopted or executed as staff member's electronic signature.
- Abide by the Agency's Environment of Care policy section on "security management" addressing issues regarding protection of paper-based and electronic health records and internet service provider outage.
- Loss and/or theft of the clinical record shall be reported immediately, followed by the completion of an incident report (See Incident Reporting Policy and Procedure). Staff shall also follow the Agency's Breach Notification Policy and Procedure in accordance with HIPAA and applicable state law.
- Use a client's EHR in an authorized manner accessing information appropriate for one's role at the Agency;
- Take appropriate steps to prevent the unauthorized re-disclosures of released information, including stamping released documents with 42 CFR, Part 2 - Confidentiality Statement and the Do Not Re-Release Statement (See Release of Information Policy and Procedure);
- Recognize that although the Agency "owns" the clinical record, the client has the right to have access to information contained in it (See Release of Information Policy and Procedure).

2. Access to the Clinical Record

- The Medical Records staff is responsible for outside requests for information.
- Individuals will have access to clinical data and the clinical record under the following circumstances/specifications:
    a. Staff who have a direct need for accessing clinical information, whether it be for clinical or billing purposes;
    b. The client;
    c. A youth/child client's parent, provided such access is not restricted by court order, applicable law, or clinical safety concerns (e.g., suspected abuse or neglect);
    d. A legal guardian that has provided the Agency with documentation of his or her legal guardian status with respect to the client;

e. Individuals where there is a release of information signed by the adult client/parent/legal guardian specifying access to specific clinical data;
f. Court/legal/law enforcement sources that provide appropriate documentation (including a valid court order, subpoena, or other legally sufficient process) as it relates to any court imposed treatment/intervention, or any civil, criminal, or administrative investigation or proceeding;
g. Auditors of accreditation bodies, subject to applicable confidentiality agreements, qualified service organization agreements, and/or business associate agreements as required by law.

Black Box Procedure

Should a staff member indicate that they know someone who is a client of the Agency, or a client indicate that they know a staff member personally, that staff member will be black boxed from the client's chart. If a staff member is also a client of the Agency, they will be black boxed from accessing their own chart in Carelogic. The staff member can contact the 'Black Box' Distribution List directly to have this completed. Additionally, if a client passes away, the following individuals will be given logged access for a period necessary to complete clinical, billing, and administrative obligations: President and CEO, Chief Operating Officer, Performance Improvement Director, EHR System Administrator, Billing Supervisor, Medical Director, Medical Records Specialist, Clinical Directors. All other Agency staff will be restricted from accessing the chart, unless otherwise approved by the Chief Operating Officer, or designee. Access by the deceased client's personal representative shall be handled in accordance with HIPAA and applicable state law.

For more details, please see the Carelogic Manual.

B. Limitations to Confidentiality

A Release of Information must be signed to release confidential information unless the information being released is identified under a limitation of client confidentiality:

- Federal laws and regulations do not protect any threat to commit a crime, any information about a crime committed by a client either at the Agency or against any person who works for the Agency;
- Federal laws and regulations do not protect any information about suspected child abuse or neglect from being reported under state law to appropriate state and local authorities (Staff Abuse and Neglect Policy and Procedure);
- Federal laws and regulations do not protect any client's threat to harm and/or intent to harm themselves or others. The Agency shall take appropriate steps to warn or protect identifiable potential victims in accordance with applicable state and federal law;
- Federal laws and regulations do not protect any information in relation to the
- reporting of communicable diseases;

- Federal laws and regulations do not protect any information about suspected animal cruelty, neglect, or abandonment, to the extent disclosure is required by applicable state law.

C. Notice of Privacy Practices

Agency clients are informed of ways in which their personal health information, clinical data and the clinical record will be used during the intake process. Clients are provided with a Notice of Privacy Practices handout detailing Agency practices, and the Agency shall make a good-faith effort to obtain written acknowledgment of receipt. Clients are also given an opportunity to ask additional questions and/or contact the RH Privacy Officer.

D. Amending/Altering the Clinical Record

1. Agency staff shall not alter or destroy an entry in the clinical record. Instead, they will cross out the entry, designate it as an error and initial and date next to the entry for paper-based records.
2. The staff shall enter a new entry showing the correct data. Agency staff may amend the clinical record when significant clinical data was not entered in the original documentation.
3. Agency clients may request to amend or add an addendum in response to data/information written in the clinical record.

E. Paper Based Clinical Records (Storage, Removal and Destruction of)

1. The storage of clinical records will be maintained in accordance with 42 C.F.R., Part 2, the HIPAA Security Rule, and applicable state law.
2. Clinical records will be stored securely at all times.
3. The Medical Records staff is responsible for the organization of the clinical record and chart room area.
4. Overflow boxes will be stored behind locked doors accessible only to Agency staff.
5. Removal of the clinical record from Agency premises is permitted only under the following circumstances and in accordance with the Agency's Chart Obtainment Policy and Procedure:
   - The transporting of the clinical record to an Agency satellite site for the purpose of service delivery, quality of care, record documentation, etc.
   - The record is needed for mandatory legal reasons and the executive director or his/her designee has authorized the removal from Agency premises.
   - The Agency staff has verified the removal of the clinical record with and received authorization from the executive director or his/her designee.
6. Upon the removal of the clinical record from Agency premises, the clinical record will be supervised and secured at all times.
7. Destruction of the Clinical Record
   - Clinical records shall be destroyed to maintain confidentiality as required by state

and federal law. Paper clinical records are destroyed by shredding, and electronic clinical records are destroyed through secure deletion or media destruction methods in accordance with applicable laws. The Medical Records staff is responsible for overseeing the efficient and secure destruction of clinical records.

- Adults: Adult clinical records shall be maintained for at least ten years following the client's discharge from the agency, or longer if required by applicable law or regulation. The destruction of the clinical record following this time frame is permitted, provided no litigation hold, regulatory investigation, or other legal obligation requires continued retention.
- Children/Youth: Children/Youth clinical records shall be maintained for at least ten years following the attainment of their eighteenth birthday, or longer if required by applicable law or regulation. Following this time frame, the destruction of their clinical record from when they were a minor is permitted, provided no litigation hold, regulatory investigation, or other legal obligation requires continued retention.
- Accidental destruction of a chart (partial or entire chart) will be documented in an incident report (See Incident Reporting Policy and Procedure). Client information will be replicated as much as possible.

Ravenwood Health must adhere to this policy and procedure. Violation of this policy and procedure is grounds for disciplinary action, up to and including termination of employment and criminal or professional sanctions.

Paul Bolins
President and CEO

11/10/2026
Date