**RAVENWOOD HEALTH**

**SUBJECT: HIPAA Compliance Policy: Employee Responsibilities** **Policy and Procedure: #509**

**EFFECTIVE DATE: 08/21/2025** **REVIEW DATE: 10/27/2026**
**BOARD APPROVAL: 08/21/2025** **Next Review Date: 10/27/2028**

**Policy:**
Ravenwood Health (the "Agency") is committed to ensuring the privacy and security of all Protected Health Information (PHI). Therefore, all Agency employees are required to comply with the Health Insurance Portability and Accountability Act (HIPAA) regulations governing privacy, security, and permissible disclosure of PHI. Staff must uphold the confidentiality, integrity, and availability of client information encountered through their job duties at the Agency. Unauthorized access, use, or disclosure of PHI is strictly prohibited.

**Purpose:**
This policy outlines the responsibilities of Agency staff in complying with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and applicable standards from the Ohio Department of Mental Health and Addiction Services (OhioMHAS) and The Joint Commission. It ensures protection of individuals' health information across all programs, including behavioral health, substance use disorder services, primary care, and youth/adult residential services.

**Scope:**
This policy applies to all staff, contractors, interns, and volunteers across all Agency programs and locations.

**Employee Responsibilities:**

General Compliance
- Adhere to all HIPAA-related policies and Agency procedures
- Protect all client information from unauthorized access or disclosure
- Immediately report any suspected HIPAA violation or data breach to the Privacy Officer or designated supervisor
- Understand and observe the "Minimum Necessary" standard, accessing only the information necessary to perform job functions. Staff working with substance use disorder (SUD) records must also comply with the additional confidentiality requirements of 42 CFR Part 2, including restrictions on redisclosure without specific patient consent.

Confidentiality and Conduct
- Do not view, share, or discuss client information unless it directly pertains to your job duties
- Refrain from accessing records of clients who are friends, family members, co-workers, or community members unless part of authorized job duties
- Do not discuss client information in public areas (e.g., break rooms, hallways, restrooms, or off-site locations)
- Avoid printing or writing down client information unnecessarily

Technology Use and Electronic PHI
- Use only secure, Agency-approved systems for storing, accessing, and transmitting PHI

- Log out or lock computers and devices when unattended
- Do not share passwords or access credentials
- Do not store PHI on personal devices or removable media unless expressly authorized by the Privacy Officer and secured with Agency-approved encryption
- Use encryption when transmitting PHI electronically outside the organization

Physical Security

- Keep client files and documents in locked storage when not in use
- Do not leave paper records, printed materials, or devices containing PHI unattended
- Dispose of paper records containing PHI using approved shredding or confidential destruction methods

Communication

- Use only approved communication platforms for client-related discussions
- Never use personal email, text messaging, or social media to transmit or discuss client information
- Never post about clients on any social media platform, even anonymously

**Reporting Violations**

All staff are required to report:

- Unauthorized access, use, or sharing of PHI
- Lost or stolen devices that may contain PHI
- Observation of any situation that may compromise data privacy or security

Reports must be made within 24 hours of discovery to the Privacy Officer or Compliance Officer. Timely internal reporting is critical to ensure the Agency can meet its obligations under the HIPAA Breach Notification Rule (45 CFR 164.400-164.414), including notification to the U.S. Department of Health and Human Services and affected individuals. Reports may also be made to an immediate supervisor, who must then promptly notify the Privacy Officer or Compliance Officer within the same 24-hour window. Reports may be made anonymously.

Ravenwood Health prohibits retaliation against individuals who report privacy concerns in good faith.

**Enforcement and Disciplinary Action**

Any individual covered by this policy (including employees, contractors, interns, and volunteers) found to have violated HIPAA standards or this policy is subject to disciplinary or corrective action, including but not limited to:

- Verbal or written warning
- Suspension or reassignment
- Termination of employment, contract, or engagement
- Referral to professional licensing boards or legal authorities, if applicable

The severity of the consequence will depend on the nature and impact of the violation. Documentation of all violations and corrective actions will be maintained.

## Policy Review

This policy will be reviewed annually by the Compliance Officer and updated as needed to remain consistent with federal and state laws, Joint Commission requirements, and OhioDBH standards.

## References

- HIPAA Privacy Rule (45 CFR Part 164, Subpart E)
- HIPAA Security Rule (45 CFR Part 164, Subpart C)
- HITECH Act
- 42 CFR Part 2 (Confidentiality of SUD Patient Records)
- Ohio Administrative Code 5122-26-03 and 5122-27-01 through 5122-27-06
- The Joint Commission: Information Management and Record of Care Standards
- U.S. Department of Health & Human Services – www.hhs.gov/hipaa

Paul Bolen 11/10/2024

President and CEO Date