ICANS Security Safeguards Policies

SCOPE AND AVAILABILITY
These policies apply to all Agencies/Authorized Users who have registered with and are participating in ICANS.

A. DEFINITIONS

Agency. A Covered Entity (agency/organization/individual) or a Business Associate of a Covered Entity as defined under HIPAA and entering into an ICANS Agency Agreement with DBH.

Authorized User. An individual designated by an Agency or DBH as having job duties necessitating access to ICANS and meeting the conditions specified in Section 5 of the Agency Agreement.

ICANS. A secure, electronic, Internet-based, EHR system is used to administer and manage CANS assessments in Idaho.

Protected Health Information. Protected Health Information means any information created for or received from an Individual under the ICANS Informed Consent from which the identity of an Individual can reasonably be determined, and includes, but is not limited to, all information within the statutory meaning of “Protected Health Information” (45 CFR § 160.103). Protected Health Information includes information maintained or transmitted in any form, electronic or otherwise.

B. COMPLIANCE WITH LAW AND POLICY

Purpose
This Policy describes DBH’s expectations in the areas of administrative, technical, and physical safeguards. HIPAA regulations provide some specifics regarding what the Federal Government requires in the area of safeguarding PHI.

POLICY:
1. Laws. Each Agency is responsible to maintain appropriate administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of PHI pursuant to HIPAA standards and CFR 42. Efforts to safeguard PHI must be appropriate to the situation and in regard to effort and expense. Participants administratively responsible for handling PHI shall ensure their processes and practices are in compliance with the HIPAA security rule and ICANS policies and standards.
2. **Agency Responsibility.** Each Agency shall have appropriate organizational policies in regard to protecting the privacy of PHI. The direct responsibility to comply with this Policy resides with the Agency. Owners of the non-ICANS electronic and paper systems containing PHI bear the responsibility for any labor or expenses associated with bringing their systems and processes into compliance with these Policies and the HIPAA security rule.

C. **TECHNICAL REQUIREMENTS**

**Purpose**
This Policy relates to the technology associated with protecting PHI.

**POLICY:**
Technical aspects associated with ensuring the privacy and security of PHI may require the expertise of information technology professionals. In those situations, the Agency is responsible for acquiring expertise to ensure the privacy and security of PHI.

D. **AGENCY RESPONSIBILITIES**

**Purpose**
This Policy addresses the expectations DBH holds for each Agency regarding end user (Authorized User) responsibilities to ensure security safeguards are in place for PHI.

**POLICY:**
1. **Authorized User.** The Agency shall comply with Section 5 of the ICANS Agency Agreement.

2. **ICANS Access.** Every Authorized Users granted access to ICANS shall have a personal login and password. The login and password provides authorization and authentication for ICANS access. Logins and passwords shall not be shared. Authorized Users must log out of or “lock” their computer systems when not in use to reduce the risk of improper access to ICANS.

3. **Termination of Access.** Covered Entities shall immediately DBH when an individual is removed from their list of Authorized Users. The notification must occur within twenty-four (24) hours of the Authorized User’s termination.

4. **Security Audit Log.** DBH shall maintain a security audit log or chronological record of system activities to enable the reconstruction, review, and examination of access to records in ICANS. If DBH has reasonable cause to believe that the Agency/Authorized User access of the system is not in compliance with Policy, DBH shall have the right to conduct an audit of transactions.

5. **Data Transmission.** Data transmitted via the Internet using ICANS is encrypted according to industry-accepted methods.
6. **Physical.** Covered Entities shall restrict access to the physical location of computers used to access ICANS.

7. **Discipline for Non-Compliance.** Each Agency shall implement procedures to hold workforce members, agents, and contractors with Authorized Access to ICANS accountable for compliance with ICANS Security Safeguards policies. Such procedures shall also include disciplinary measures for non-compliance. Disciplinary measures may include verbal or written warnings, demotion, suspension, or termination. DBH reserves the right to terminate Agency/Authorized User access based on the non-compliance with ICANS Policies.