ICANS Privacy Policies

INTRODUCTION
These Privacy Policies apply to the access, use and disclosure of protected health information by registered Agencies/Authorized Users with access to ICANS. These policies will be reviewed and revised as needed based on changes to State or Federal law or regulations.

These Policies combined with the privacy policies and procedures already established and implemented by Agencies/Authorized Users under HIPAA, form a comprehensive array of administrative safeguards addressing privacy of protected health information.

The goal is to promote a balance between consumer control of and access to health information with the need of participating Agencies/Authorized Users to access that information to ensure the quality and coordination of care.

EFFECT OF LEGISLATION AND RULE CHANGES
DBH and Agencies/Authorized Users need to remain flexible in approach to adapt to the uncertainty of state and federal legislation and regulations that will affect design, safeguards, rights and responsibilities over time.

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

A. DEFINITIONS

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

Agency Agreement. A legally binding agreement between DBH and an Agency. Under the ICANS Agency Agreement, DBH registers the Agency in accordance with the Terms and Conditions of the Agency Agreement.

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 7 (Authorized Users).

Authorized User Agreement. A legally binding agreement between DBH and an Authorized User. Under the ICANS Authorized User Agreement, DBH registers the
Authorized User in accordance with the Terms and Conditions of the Authorized User Agreement.

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

**Individual.** An individual with a signed Idaho CANS Informed Consent.

**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 stipulates compliance with all applicable laws and ICANS policies.

**POLICY:**

1. **Laws.** Each Agency/Authorized User shall, at all times, comply with all applicable federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of individually identifiable health information and establishing certain individual privacy rights.

2. **ICANS Policies.** Each Agency/Authorized User shall, at all times, comply with all applicable ICANS policies and procedures. The ICANS eManual sets forth the policies and procedures under which DBH shall provide ICANS. Each Agency/Authorized User is responsible for ensuring it has, and is in compliance with, the most recent version of these ICANS Policies.

3. **Agency/Authorized User Policies.** Each Agency/Authorized User is responsible for ensuring that it has the requisite, appropriate, and necessary internal policies for compliance with applicable laws and these ICANS Policies. In the event of a conflict between these ICANS Policies and an organization’s own policies and procedures, the Participant shall comply with the Policy that is more protective of individual privacy and security.

### C. NOTICE OF PRIVACY PRACTICES

**Purpose**

This Policy relates to the maintenance of privacy notices.

**POLICY:**

Each Agency/Authorized User shall develop and maintain a notice of privacy practices
(the Notice) that complies with applicable law and this Policy.

1. **Content.** The Notice shall meet the content requirements set forth under the HIPAA Privacy Rule and comply with all applicable laws and regulations. For Agency/Authorized User that are also health care providers, the Notice shall inform clients that their health information will be entered in ICANS. The notice will also advise clients to the right to restrict disclosure of health information through the ICANS.

2. **Provision to Clients.** Each Agency/Authorized User shall have its own policies and procedures governing distribution of the Notice to Individuals, which shall be consistent with this Policy and comply with applicable laws and regulations.

**D. INDIVIDUAL AND CONTROL OF INFORMATION**

**Purpose**
This Policy addresses an individual's choice to restrict information after it is entered in ICANS.

**POLICY:**

1. **Choice to Restrict Future Disclosures.** Every Individual has the right to limit Agency/Authorized User access to health information about him or her after the information is entered in ICANS. Unless an Individual completes the process to limit Agencies/Authorized Users’ access to information about the individual through ICANS, the information on that individual may be made accessible to all Agencies/Authorized Users with access to ICANS.

2. **Request to Restrict Notification.** Agencies shall establish reasonable and appropriate processes to enable the exercise of the Individual's choice not to have information about him or her made accessible to Agencies/Authorized Users through ICANS. The methods described in this Policy are not exclusive, and Agencies may adopt additional, not inconsistent, processes.

3. **Submission of a Request to Restrict Access.** An Individual choosing to restrict Agencies/Authorized Users’ access to his or her ICANS information must submit a request to restrict information to the Agency. The Agency will submit the request to restrict information to DBH.

4. **Effect of Choice.** DBH shall implement appropriate mechanisms to securely prevent access to clinical information about an individual when requested to do so. A decision to restrict access only affects the availability of the Individual's protected health information through the ICANS. An Authorized User who queries an Individual who has requested a restriction will not be able to view any information entered in ICANS for the Individual.

A request for a restriction affects all Agencies/Authorized Users’ future access to the Individual’s information not just with respect to an Agency or episode of care.
5. **Revocation.** An Individual may revoke a prior election to restrict data at a later date. No information regarding an Individual who has requested ICANS not share information with Agencies/Authorized Users shall be made accessible through ICANS unless or until the individual revokes his or her decision. The request to rescind the choice to have ICANS restrict information must be submitted to the Agency. The Agency will submit the request to rescind the restriction to DBH. Information on the Individual can be made accessible in ICANS, effective the date he or she requests to revoke the restriction.

Withdrawing a restriction will result in information that was previously unavailable through ICANS becoming available to all Agencies/Authorized Users.

6. **Documentation.** DBH must maintain the documentation for all individuals choosing not to have information about them accessed through ICANS.

Once a restriction request has been processed, an acknowledgement letter will be sent to the individual confirming receipt of and action on the request by the Agency.

Once a request to revoke a restriction has been processed, an acknowledgement letter will be sent to the individual confirming receipt of and action on the request by the Agency.

Documentation of all requests and acknowledgement letters must be retained for six (6) years.

---

**E. USES AND DISCLOSURES OF HEALTH INFORMATION**

**Purpose**

This Policy addresses limitations on the use of information, accountability, and oversight.

**POLICY:**

1. **Compliance with Law.** All disclosures of health information through ICANS and the use of information obtained from ICANS shall be consistent with all applicable federal, state, and local laws and shall not be used for any unlawful discriminatory purpose.

2. **Purposes.** Uses and disclosures of health information through ICANS shall be for the purpose of behavioral health care treatment, as permitted by applicable laws and regulations. Each Agency/Authorized User shall provide or request health information through ICANS only to the extent necessary via Agency/Authorized User security profiles and only for those purposes that are permitted by applicable federal, state, and local laws and regulations and these Policies. Information shall not be requested for marketing or marketing related purposes. Under no circumstances shall information be requested for a discriminatory purpose. In the absence of a permissible purpose, an Agency/Authorized Use shall not request information through ICANS.
3. **Agency/Authorized User Policies.** Each Agency/Authorized User shall refer to and comply with its own internal policies and procedures regarding disclosures of health information and the conditions that shall be met and documentation that shall be obtained, if any, prior to making such disclosures.

4. **Access Logs.** ICANS shall maintain an access log. The access log is a list of all individual files requested from ICANS. The access log may be used to conduct periodic audits. Participants will be provided the results of these audits upon request. The access log can be monitored for inappropriate access. If inappropriate access is identified, reported or suspected, the incident will be investigated.

5. **Authentication.** Each Agency/Authorized User shall follow uniform minimum authentication requirements as specified in ICANS Security Safeguards Policy for verifying and authenticating those within their organizations who shall have access to, as well as other Agency/Authorized User who request access to, information through ICANS.

**F. MINIMUM NECESSARY**

**Purpose**
This Policy incorporates the HIPAA privacy rule requirements that Agencies shall disclose only the amount of information reasonably necessary to achieve a particular purpose.

**POLICY:**
1. **Uses.** Each Agency/Authorized User shall access through ICANS only the minimum amount of health information necessary for the purpose of such use. Access to health information obtained through ICANS shall be limited to workforce members, agents, and contractors who need the information to perform their job function or duties.

2. **Requests.** Each Agency/Authorized User shall request only the minimum amount of health information through ICANS as is necessary for the intended purpose of the request.

**G. AUTHORIZED USERS**

**Purpose**
This Policy addresses legitimate use of health information, proper implementation of Agencies/Authorized Users’ privacy practices, prompt identification of privacy violations and the undertaking of remedial action for those violations.

**POLICY:**
1. **System Access.** Each Agency shall request access to ICANS for only those workforce members, agents, and contractors who have a legitimate business need to use ICANS to release or obtain information. Prior to being granted access to ICANS, any workforce member, agent, or contractor must meet the
criteria outlined in Section 5 of the ICANS Agency Agreement.

Agencies must maintain appropriate administrative, technical, and physical safeguards to prevent any unauthorized use or disclosure of PHI pursuant to HIPAA standards.

2. Training. Each Agency shall ensure its workforce members, agents, and contractors who will have access to ICANS are provided training on these Policies. Each trainee must confirm an acknowledgement that he or she has received, read, and understands these Policies.

3. Discipline for Non-Compliance. Each Agency shall implement its own procedures to hold workforce members, agents, and contractors accountable for ensuring that they do not use, disclose, or request health information except as permitted by these Policies and they comply with, but are not limited to these Policies. Such procedures shall also include disciplinary measures for non-compliance with these Policies. Such disciplinary measures may include verbal or written warnings, fines, demotion, or termination. ICANS reserves the right to terminate Authorized User access based on non-compliance with ICANS Policies.

4. Reporting of Non-Compliance. Each Agency shall have a mechanism for reporting any non-compliance with these Policies, and shall require all workforce members, agents, and contractors to report any non-compliance with these Policies to the Participant. Agencies shall also investigate and take appropriate corrective action on any internally reported non-compliance with these Policies. Agencies shall notify DBH regarding instances of significant non-compliance.

5. Follow up On Audit Findings. Each Agency shall follow up on ICANS audit findings of alleged inappropriate use. Each Agency must have a corrective action process in place for handling any non-compliance with these Policies by its workforce members, agents, and contractors.

H. MITIGATION

Purpose
This Policy applies to all Agencies that are registered with and are participating in ICANS and that may provide, make available, or request PHI through ICANS.

POLICY:
1. Participant Responsibility. The Agency is responsible to mitigate any breach or improper disclosure of PHI committed by the Agency/Authorized Users, in accordance with laws, rules, regulations, or guidelines established by state or federal regulations.

2. DBH Responsibility. DBH is responsible to mitigate any unsecured (unencrypted) breach or improper disclosure of PHI committed by DBH Authorized Users in
accordance with laws, rules, regulations, or guidelines established by state or federal regulations.

3. **DBH Process.** DBH will develop a process to mitigate a breach or improper disclosure, etc. Mitigation includes appropriate remedial action to limit to the extent practicable, any harmful effect of the breach, failure or improper disclosure - which may include a request to the party who received such information to return and/or destroy the impermissibly disclosed information. DBH must also provide the particulars of an unsecured (unencrypted) PHI breach as well as a comprehensive list of all the individuals whose information was breached or suspected of being breached to the Agencies(s) involved. The Agencies(s) are then responsible to provide notification to the individual(s) of the disclosure of information about them and to follow all other state or federal regulations applicable to such breach or incident.