

Idaho Health Data Exchange Security Safeguards Policy

Scope and Availability

This Security Safeguards Policy applies to all Participants who have registered with and are participating in the Idaho Health Data Exchange and that provide, make available, or request health information through the Idaho Health Data Exchange.

Definitions

Idaho Health Data Exchange (IHDE). “Idaho Health Data Exchange (IHDE)” shall mean a secure electronic Health Information Network in the State of Idaho.

Organization. “Organization” shall mean any individual or group of individuals registered with and participating in the IHDE that may provide, make available, or request health information through the IHDE.

Participant. “Participant” shall mean a member within the networked environment of the Idaho Health Data Exchange including health care institutions and professionals, labs, payers, etc. that have current Contracts and Data Sharing Agreements with the IHDE.

Protected Health Information (PHI). “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 C.F.R. § 160.103 and 164.501, limited to the information created or received by IHDE from or on behalf of the Participant.

Compliance with Law and Policy

Purpose

This policy describes IHDE’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.** The Participant is responsible to maintain appropriate administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of PHI pursuant to HIPAA standards found at 45 C.F.R. § 164.530(c). 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 IHDE policies and standards.

2. **Responsibility.** The Participant shall have appropriate organizational policies in regard to protecting the privacy and security of PHI. The direct responsibility to comply with this Policy resides with the Participant. Owners of the non-IHDE electronic and paper systems containing PHI bear the responsibility for any labor and/or expenses associated with bringing their systems and processes into compliance with these Policies and the HIPAA security rule.

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 Participant is responsible for acquiring expertise to ensure the privacy and security of PHI.

Participant Responsibilities

Purpose

This Policy addresses the expectations the IHDE holds for each Participant regarding end user responsibilities to ensure security safeguards are in place for PHI.

POLICY:

1. **User Authentication.** Participants must have an account creation process to grant workforce members, agents and contractors access to the IHDE. Access to the IHDE or systems connected to the IHDE shall be granted only after the account creation process has been completed.

Components of the account creation process shall include positive identification of the individual, determination of the person's roles and access requirements, training of the individual regarding proper use of the account and IHDE policies, as well as written acceptance of IHDE and Participant level policies regarding appropriate use of the resources.

2. **Account Access.** Every Participant user granted access to the IHDE shall have a unique username and password. Group logins are not allowed. Users must log out of or "lock" their computer systems when not in use to reduce the risk of improper access to the IHDE.

3. **Security Audit Log.** IHDE shall maintain a security audit log or chronological record of system activities to enable the reconstruction, review and examination of access to records in the IHDE. If the IHDE has reasonable cause to believe that the Participant user access of the system is not in compliance with these Policies, IHDE shall have the right to conduct an audit of transactions and access to records in the IHDE.
4. **Data Transmission.** Data transmitted via the Internet using the IHDE shall be encrypted according to industry-accepted methods.
5. **Fax Machines.** Fax machines used to receive information from the IHDE shall be placed in locations secured from the public.
6. **Physical.** Participants shall restrict access to the physical location of computers used to access the IHDE.
7. **Discipline for Non-Compliance.** Each Participant shall implement procedures to hold workforce members, agents, and contractors accountable for compliance with IHDE 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. The IHDE reserves the right to terminate Participant user access based on non-compliance with IHDE Policies.