




Immunization Unit
 Public Health Division
 122 West 25th St. 3rd Floor West
 Cheyenne, WY 82002
 307-777-7952 • Fax 307-777-3615
 www.health.wyo.gov



Stefan Johansson
 Director

Mark Gordon
 Governor

Policy Title:	IIS Authorized User	
Policy Number:	IMM-003	
Effective Date:	November 1, 2017	
Modified Date:	February 6, 2024	
Approval:	 Stephanie Pyle, MBA Senior Administrator, Public Health Division	<u>2-21-24</u> Date

Purpose: This policy establishes the criteria and conditions by which an individual may be granted access to the Immunization Information System (IIS) adopted by the Wyoming Department of Health (WDH) for the purpose of protecting patient information and to prevent unauthorized access to the IIS or the data contained therein.

Definitions:

“Authorized user” means an individual who is employed by an organization and for whom access to the IIS has been requested and granted.

“Facility” means any location providing medical services to people and owned or operated by an organization.

“Immunization information system (IIS)” means a confidential, computerized information system that collects vaccination or immunization data about individuals that has been established and is managed by the WDH.

“Organization” means an establishment that has enrolled with the WDH to access the IIS.

“Security incident” As stated in 45 CFR § 164.304 means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Policy:

1. Identification

- a. A facility contact may request for an individual to become an authorized user using the forms and processes established by the Immunization Unit.
- b. An individual is eligible to become an authorized user if the individual:
 - i. Is a current employee of an organization.
 - ii. The Immunization Unit approves the individual to become an authorized user following verification of eligibility and the source of the request.

- iii. The Immunization Unit shall assign the authorized user an access level in accordance with this policy.

2. User Access

- a. Role-based access will be determined using the “minimum necessary principle” to limit disclosure of protected health information based on the authorized user’s official duties.
- b. Access will be requested by the organization or facility contact and assigned by the Immunization Unit.

3. Authentication and Revocation

- a. Authorized users must maintain a unique email address, username, and password.
- b. Password management in the IIS is established in accordance with WDH policies.
- c. Unauthorized users shall be denied access.
- d. Organization or facility contacts must notify the Immunization Unit to inactivate authorized users that are no longer associated with the organization.
 - i. Notification of inactivation must be received as soon as the need for inactivation has been identified; however, no more than one (1) calendar day after.
- e. Routine revocation of access shall occur after 30 days of inactivity.
 - i. In order to reinstate access, follow the procedures and processes outlined on the Immunization Unit website at <https://health.wyo.gov/publichealth/immunization/>.

4. Security Incidents

- a. Security incidents involving the IIS or data contained therein shall be immediately reported to the Immunization Unit at wyr@wyo.gov using ‘urgent’ in the subject line. The Immunization Unit will complete necessary documentation and reporting in accordance with WDH policies.
- b. Security incidents include but are not limited to:
 - i. Unauthorized disclosure of IIS data;
 - ii. Theft of IIS data;
 - iii. Unauthorized use of IIS data;
 - iv. Unauthorized data access;
 - v. Misuse of confidential information;
 - vi. Spyware detection;
 - vii. Virus detection;
 - viii. Electronic transmission of sensitive IIS data without use of data encryption mechanism; and
 - ix. Electronically transmitted threats to WDH IIS staff, equipment, infrastructure, etc.
- c. In addition to security incidents, authorized users who have reason to believe that their personal information or IIS data have been compromised or that computer intrusion or tampering has occurred with respect to their accounts, shall email details of the concern or incident using ‘urgent’ in the subject line to wyr@wyo.gov immediately.

- d. Security incidents may be identified through WDH conducted audits as per IIS Audits Policy (IMM-007).

5. Security Incidents: Penalties and Remedies

- a. Corrective action may be taken against an authorized user who has been involved in a security incident per the IIS Security Incidents: Penalties and Remedies Policy (IMM-008).
- b. An authorized user's access to the IIS may be suspended or terminated if the authorized user violates the requirements outlined in this policy.

Contacts:

Immunization Unit Main Line	307-777-7952
Immunization Unit Manager	307-777-6001
Immunization Registry Records and Data Manager	307-777-8503

References:

45 CFR § 164.304
WDH Immunization Program Administrative Rules and Regulations
IIS Audits Policy (IMM-007)
IIS Security Incidents: Penalties and Remedies Policy (IMM-008)
Immunization Unit Processes and Procedures