Wyoming Department of Health

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 Security Incidents: Penalties and Remedies
Policy Number:	IMM-008
Effective Date:	February 6, 2024
Approval:	Stephanie Pyle Stephanie Pyle, MBA Senior Administrator, Public Health Division 2-21-24 Date

Purpose: This policy establishes the penalties and remedies for unauthorized use of the Wyoming Department of Health (WDH), Immunization Information System (IIS) by authorized users.

Definitions:

"Authorized User" means an individual who is employed by an organization and for whom access to the IIS has been requested and granted.
"Organization" means an establishment that has enrolled with the WDH to access the IIS.
"Responsible Authority" means an individual with signatory authority to enter into contractual agreements on behalf of an establishment, organization, school, or child caring facility and is responsible for the conditions outlined in the Information Sharing Agreement (ISA).
"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. **Security Incidents**
    a. Suspected security incidents shall be immediately reported to the Immunization Unit through email using "urgent" in the subject line to wyir@wyo.gov. Security incidents may also be identified through routine audits pursuant to IIS Audits policy (IMM-007).
        i. The Immunization Unit will complete necessary documentation and reporting in accordance with WDH policies.
        ii. The Immunization Unit will notify the Responsible Authority.
    b. The Immunization Unit shall immediately suspend an authorized user's IIS access pending an investigation of any authorized user who is suspected of a security incident.

c. The Immunization Unit will terminate the authorized user's account permanently if security incidents are substantiated as malicious.
d. Security incidents that are determined to be without malicious intent shall be addressed as follows:
    i. Upon first security incident, the Immunization Unit will provide a copy of the Penalties and Remedies Review Checklist, WDH Immunization Program Administrative Rules and Regulations, the IIS Authorized User Policy (IMM-003), and the IIS End User License Agreement (EULA). The Penalties and Remedies Review Checklist will be required to be submitted to the Immunization Unit as written confirmation of review.
    ii. Upon a second security incident, the Immunization Unit will suspend the authorized user's account for 30-days.
    iii. Upon the third security incident, the Immunization Unit will permanently terminate the authorized user's account and deny future requests for a user account.

2. Immunization Unit Responsibilities

a. The Immunization Unit shall:
    i. Require each organization to have a mechanism for all authorized users to report any non-compliance of Immunization Unit policies to the organization and Immunization Unit, as soon as the security incident is identified.
    ii. Conduct audits to review use and require organization and authorized user compliance.

Contacts:

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

Forms:

IIS Penalties and Remedies Review Checklist

References:

45 CFR § 164.304
WDH Immunization Program Administrative Rules and Regulations
IIS Authorized User Policy (IMM-003)
IIS Audits Policy (IMM-007)
IIS End User License Agreement (EULA)
IIS Penalties and Remedies Review Checklist
Immunization Unit Processes and Procedures