Security Policy

Hawaii State Immunization System (HiSIS)

March 2025

I. Introduction

A. The Hawaii State Immunization System, hereinafter referred to as "the Registry" or "Registry" or “Registry System” or “System”, is a statewide web-based immunization information system that establishes and maintains a repository of lifespan immunization data for the population of the State of Hawaii. The Registry was developed through the efforts of the last Hawaii Immunization Registry Coalition, which was composed of over 70 representatives from health-related organizations statewide and was overseen by the Department of Health Immunization Branch, hereinafter referred to as "the Immunization Branch" or "Immunization Branch."

B. The Registry is a computerized system that ensures the secure, electronic exchange of immunization information to:
   1. Aid immunization providers in ensuring that their clients are appropriately immunized, thereby increasing immunization rates in Hawaii.
   2. Provide the data necessary to plan, coordinate, and promote efficient and cost-effective communicable disease prevention and control efforts

II. Purpose

A. This document hereinafter referred to as “Security Policy” or “Policy,” shall govern the administrative, physical, and technical safeguards of the Registry System to protect the confidentiality, integrity, and availability of its data. Implementation of these safeguards is intended to reduce the risks and minimize the effects associated with the unauthorized access, alteration, deletion, and transmission of data collected and maintained in the Registry while in use and when stored.

B. All authorized users and the Immunization Branch acknowledge that the Health Insurance Portability and Accountability Act (HIPAA) Security Standards; Final Rule (45 CFR Parts 160, 162, and 164, “Health Insurance Reform”) govern the security of individually identifiable health information electronically stored or transmitted by entities subject to the Security Rule. HIPAA standards for security were used as a guide to assist in the development of this document. Providers, health plans, and other covered entities who are authorized users shall comply with the HIPAA Security Standards. Although the Registry and the Immunization Branch are not covered entities under HIPAA, the Immunization Branch shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Registry System.

1. Administrative Safeguards

a. Administrative Safeguards involve the management of day-to-day operations, conduct of, and access by persons utilizing the Registry System, and development of security activities and countermeasures in response to risks to Registry operations.

b. The Registry System shall operate in accordance with all applicable federal and state laws and regulations that govern security of individually identifiable health information (IIHI), including but not limited to:
   1. Hawaii Revised Statutes §§325-121 through 325-126, “Immunization Registry”
   2. HIPAA Security Standards; Final Rule (45 CFR Parts 160, 162, and 164, “Health Insurance Reform”)
   3. Hawaii Revised Statutes §487J, “Social Security Number Protection”
   4. Hawaii Revised Statutes §487N, “Security Breach of Personal Information”
   5. Hawaii Revised Statutes §487R, “Destruction of Personal Information Records”

All persons requiring access to the Registry System are responsible for understanding their role in securing the System and shall comply with this Policy and all applicable federal and state laws and regulations that govern the security of IIHI.

1-A Security Management Process

The Registry Security Management Process includes security monitoring, malicious software management, configuration management, and incident response. The Registry Security Policy utilizes a Risk Analysis and Risk Management approach to address information security. This approach identifies, assesses, rectifies, and appropriately mitigates vulnerabilities and threats that can adversely affect the Registry System.

1-A-1 Risk Analysis

A risk analysis shall be performed every other year to identify potential risks/vulnerabilities to the Registry System and to determine the magnitude of impact on the Registry System, should those risks/vulnerabilities manifest. Any identified weaknesses shall be documented by the Immunization Branch and addressed by Branch initiation of the Risk Management process (see 1-A-2).

1-A-2 Risk Management

Risk management involves prioritizing, evaluating (including cost-benefit analysis), and determining whether the Immunization Branch should mitigate the risk, accept the risk with explanation, or submit a Corrective Action Plan. It shall be the responsibility of the Registry System Administrator or designee to develop and implement the most appropriate controls to decrease risk to an acceptable level with minimal adverse impact.

1-A-3 Sanction Policy

The Registry System shall not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, or for the solicitation or performance of any activity that is prohibited by any state or federal law. In addition, unauthorized creation, access, use, disclosure, modification, destruction or transmission of the Registry System and/or information contained therein is prohibited. The penalty for violation of the Registry Security Policy or any applicable federal and state laws and regulations shall include any allowable sanctions, such as termination of user access to the Registry and civil and/or criminal penalties. Violations of the Registry Security Policy shall be reported to the appropriate authorities.

1-A-4 Information System Activity Review

The Immunization Branch shall perform and document a review of system activity records (i.e. audit logs, access reports, and security incident tracking reports) every other year or whenever there is a significant change that may affect the confidentiality, integrity, security, or availability of the Registry System. Action shall be taken as appropriate.

1-A-5 Storage/Archives

The Immunization Branch shall implement archival and storage procedures to archive inactive patient records annually. System activity logs will be archived twice per year.

1-A-6 Evaluation

The Registry System, this Security Policy, and the procedures written to implement this Security Policy shall be evaluated and updated by the Immunization Branch every two years or in response to any environmental or operational changes. The evaluation shall address at minimum:

a. Risk Analysis/Assessment
b. Risk Management
c. System Activity Review

d. Security Incident Review
e. Facility Access
f. Contingency Plan
g. Transmission Security

1-B Workforce Security

1-B-1 Access

The Immunization Branch shall grant appropriate access only to authorized Registry users and shall implement procedures to prevent access to the Registry System by unauthorized persons. The Immunization Branch shall develop, implement, and enforce the policies that are addressed under the Information Access Management section.

1-B-2 Assigned Security Responsibility

The Registry System Administrator shall have the overall responsibility for the development, implementation, and enforcement of this Security Policy and procedures written to implement this Policy. The Registry System Administrator may delegate authority of any of these duties as deemed necessary.

1-C Information Access Management

1-C-1 The Immunization Branch shall authorize, establish, modify, and terminate appropriate levels of user access to the Registry via this Policy and procedures written to implement this Policy, in order to maintain the confidentiality, security, and integrity of the System.

a. Access management and support function activities shall be divided among and performed by different individuals (e.g. checks and balances, separation of duties) to ensure access security.
b. Information access management procedures shall be reviewed every other year and amended as needed to enhance security.
c. Access to the Registry shall be limited to those authorized individuals and/or entities that require regular access to client immunization and other Registry information to provide immunization services to specific clients, maintain a computerized inventory of their public and private stock of vaccines, assess immunization status to determine immunization rates, and/or ensure compliance with mandatory immunization requirements. Approval of access shall be at the discretion of the Immunization Branch.
e. Persons requesting access to the Registry shall follow the Authorized User Application Procedure (available from the Immunization Branch).
f. All accounts created shall have an authorized request and approval in accordance with the Authorized User Application Procedure (available from the Immunization Branch).
g. Each authorized user shall be assigned an account to access the Registry and shall be prohibited from sharing this account.
h. Users shall be held accountable for actions performed with their assigned account.
i. Notification of conditions for access and acceptable use (in accordance with the Registry Confidentiality and Privacy Policy and the Registry Security Policy) shall be displayed upon first successful log-on. Users shall acknowledge receipt of notification prior to gaining Registry System access.
j. Authorized users shall comply with the Registry Confidentiality and Privacy Policy, Registry User Agreement, Registry Confidentiality and Security Statement, and this Policy.
k. Permission shall be restricted by the Immunization Branch according to the

user's assigned level of access.

l. Levels of access shall include at minimum "Reader" (view only) and "User" (view, add, and modify data).

m. Authorized users shall complete the Authorized User Application procedure annually.

n. Confirmation of authorized users and access privileges shall be conducted annually and access for users not in compliance with the Authorized User Application procedure shall be inactivated in the system.

o. Termination of access shall occur at any time at the discretion of the Immunization Branch. Reasonable notice shall be given prior to termination of access.

p. Accounts that have been inactive for 90 days shall be disabled.

1-D Security Awareness and Training

1-D-1 An Information Security Awareness and Training plan shall be developed and implemented by the Immunization Branch for all persons requiring access to the Registry System. This plan shall be reviewed and updated as necessary.

a. All persons accessing or entering data via the HiSIS user interface shall complete the DOH-sanctioned security awareness training prior to gaining access to the Registry System.

b. Annual security awareness refresher training shall be provided to all identified users as appropriate.

c. Completion of the DOH-sanctioned security awareness and refresher training shall be documented.

d. All persons shall receive training and training materials appropriate to their level of access.

e. At a minimum, the training curriculum shall include: system security requirements, user responsibilities, security incident reporting, security reminders, log-in monitoring, password management, activities to circumvent social engineering, and protection from malicious software.

f. Information will be disseminated to all persons accessing the Registry System of new security items through HiSIS Announcements.

1-D-2 Password Management

All passwords for accounts shall be constructed in accordance with the following Registry password management specifications.

a. All account passwords shall expire after 90 days.

b. All stored passwords shall be encrypted.

c. Passwords shall NOT be shared.

d. Password cracking is strictly forbidden.

e. Rules for password configuration shall include at minimum:

1. Uniqueness
2. Conditions under which passwords shall be changed
3. Storage
4. Character sets
5. Length
6. Safeguarding

f. Passwords shall not include:

1. Names or dictionary words (English or foreign)
2. The user ID (e.g. if the user ID is johndoe, an invalid password is johndoe123)

1-E Security Incident Procedures

1-E-1 Incident Response (IR) Procedures

IR procedures shall be developed, disseminated, reviewed, and updated as necessary by the Immunization Branch. All security incidents, suspected incidents, and outcomes shall be documented. The IR procedures shall include at minimum:

a. Identification, containment, eradication, recovery, follow-up, response, and reporting of all security incidents and suspected incidents
b. Preservation of evidence collected pertaining to all security incidents and suspected incidents
c. On-going monitoring for security incidents
d. Periodic testing of Registry IR capabilities and effectiveness
e. Mechanism and procedures for monitoring, responding to, and reporting of all security incidents or suspected incidents
f. Identification of resources required to support the IR plan

1-E-2 Response and Reporting

In the event that a security incident results or is likely to result in unauthorized access to and acquisition of data containing IIHI, incident handling and response procedures detailed in the Registry Confidentiality Policy and HDOH Policy 26.01, "Notification of Security Breaches" shall be followed.

1-F Contingency Plan

1-F-1 The Registry Contingency Operation Plan shall be developed by the Immunization Branch in conjunction with the system vendor. Copies of the Contingency Operation Plan shall be stored in a secure location at an alternate site accessible by designated personnel. The Contingency Operation Plan shall be practiced and tested on an annual basis. The plan shall address responding to a disruption of service, and shall include at minimum:

a. A listing of key personnel roles, responsibilities and contact information
b. Identification of alternate individuals who shall be granted access in the case of a catastrophic event
c. Procedures for restoring the system after a disruption or failure
d. Disaster recovery, data back-up and system failover
e. Contingency training, plan testing and updating
f. Emergency access
g. Identification of separate routine and alternate storage and operations sites
h. Identification of alternate telecommunication services

2. Physical Safeguards

Registry physical safeguards include facility access controls limiting physical access to Registry Operations Centers, appropriate management and security of workstations used to access Registry information, procedures for controlling and tracking the handling of hardware and software, and procedures for Registry data backup, storage and disposal.

2-A Facility Access Controls

2-A-1 Access to the Registry Operations Centers shall be restricted to authorized personnel only.

a. The Registry Operations Centers shall be secured at all times and accessible to authorized persons only. Only persons with a definite need to be in the area to perform their assigned duties shall be authorized to enter.

b. The Health Information Systems Office staff shall be responsible for controlling access to the Registry Operations Centers.
c. Physical access control devices (e.g. keys, locks, combinations, or card-readers) shall be used to control entry to the Registry Operations Centers.
d. Combinations and keys shall be changed promptly when lost, compromised, or when individuals are transferred or terminated.
e. Doors shall be closed immediately after use at all times.
f. If Registry equipment has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal Registry activities, the primary user shall promptly inform the Registry Systems Administrator or designee.
g. The Immunization Branch/Health Information Systems Office shall maintain a log of repairs and modifications made to the physical components in each facility. These items include, but are not limited to:
    1. Hardware;
    2. Walls;
    3. Doors; and
    4. Locks.

2-B Workstation Use

2-B-1 All Registry authorized users are responsible for appropriate management of the workstation used to access the Registry System, including the physical area surrounding the workstation and peripheral devices including but not limited to printers and facsimile machines. The Registry System shall be used in a secure manner and only for authorized purposes.

2-B-2 Users shall **not**:
a. Install or run unauthorized or unnecessary software.
b. Download, install, or run programs or utilities that gather information to reveal/exploit weaknesses or obstruct security functions of the Registry System.
c. Make unauthorized copies of copyrighted software.

2-B-3 Workstation Security
All Registry authorized users shall take steps to protect information being stored, accessed, or processed within a workstation. Minimum activities for securing workstations, including the physical area surrounding the workstation, and peripheral devices, including but not limited to printers and facsimile machines, are as follows:
a. Workstations shall be located in a secure area.
b. Workstations shall be outfitted with appropriate electrical power conditioning, surge protection, or backup power appliances.
c. Screensavers shall be set to lock automatically after ten (10) minutes of system inactivity.
d. Screensavers shall be password protected.
e. Workstation screens shall be locked whenever a user steps away from them.
f. The monitors/screens of systems that are used to process sensitive information shall be turned/configured in a manner that does not allow over the shoulder viewing by unauthorized users.
g. Ability to boot from floppy drive or CD ROM shall be disabled.
h. The same policies for workstations apply to laptops and other mobile devices that contain confidential information; additional considerations include:
i. Extra protection such as a lockable cable, usually designed specifically for laptops, shall be used to secure the laptop at all times when unattended.
j. When traveling with a laptop that contains sensitive information, the information shall be encrypted.
k. A "clean desk" policy shall be observed; all confidential materials shall be

secured in locked drawers and desks shall be cleared if the unattended period is unknown.

l. Before exiting, the last employee to leave an office shall conduct a workspace security check of the entire office. This check shall be performed any time an office is about to be completely vacated.

m. Exception: If an office is being evacuated due to an emergency and/or disaster situation, including but not limited to fire or any other threat to life and/or property, the workspace security check shall be waived.

2-C Device and Media Controls

2-C-1 The Immunization Branch shall observe formal procedures for controlling and tracking the handling of hardware and software, and for data backup, storage and disposal. This includes the receipt, movement, and removal of hardware and electronic media that contain individually identifiable health information.

2-C-2 Disposal

a. Registry information is confidential and shall be disposed of accordingly.

b. Media destruction and disposal procedures shall be implemented in accordance with Hawaii Revised Statutes (HRS) §487R "Destruction of Personal Information Records" for both electronic and paper (where applicable), to ensure that Registry information does not become available to unauthorized persons. Department of Health personnel shall comply with the Department of Health Policy Number P27.01, "Destruction of Personal Information Records." Confidential information shall be destroyed beyond ability to recognize and recover.

c. Information shall be retained and/or destroyed in accordance with Federal regulations and the State's record retention schedule as assigned by the Department of Accounting and General Services (DAGS) Archives Division, Records Management Branch.

2-C-3 Media Re-use

a. The Immunization Branch shall follow procedures for the sanitization and re-use of storage devices and electronic media to ensure that confidential information is removed beyond ability to recognize and recover.

b. Verification of sanitized storage devices and electronic media shall be completed and documented by the Immunization Branch prior to re-use.

2-C-4 Data Backup and Storage

a. In accordance with Registry Data Backup and Storage procedures that have been written to implement this Policy, an exact copy of all Registry data shall be created following a predetermined schedule and shall be securely stored to safeguard against unauthorized access, modification or disclosure.

b. Back-up media shall be encrypted, password protected, and stored at the Department of Health and at an off-site location in locked safes or cabinets.

3. Technical Safeguards

Technical safeguards are those security mechanisms used to protect the Registry System from unauthorized access, use, disruption, modification, or destruction. The Registry System utilizes access controls to restrict permissions in accordance with an authorized user's assigned level of access, audit controls to record and monitor System activity, integrity processes to protect against improper modification or destruction, person authentication processes to verify those seeking access to the Registry System, and transmission security processes to prevent unauthorized access while Registry information is being transmitted over an electronic communications network.

3-A Access Control

3-A-1 Technical procedures (including unique user identification and emergency access procedures) shall be implemented to maintain the confidentiality and integrity of the Registry System and to allow appropriate levels of access only to authorized users.

3-A-2 Data elements to be restricted shall be identified and classified based on levels of sensitivity, confidentiality, and risk associated with inappropriate disclosure. Restricted data elements shall be non-displaying depending on user's level of access to prevent viewing by anyone who does not have permission and a need to know.

3-A-3 To avoid viewing other patients' records, an authorized user shall be required to enter predetermined patient-specific data fields to access the record.

3-A-4 Authorized users shall be assigned a unique user name.

a. Users shall not directly or by implication employ a false identity (i.e. use the name or electronic identification of another).
b. A user may use a pseudonym (an alternative name or electronic identification for oneself) for privacy or other reasons, as long as the pseudonym does not constitute a false identity.
c. Users are responsible for ensuring that that their User ID and password are not disclosed to third parties.

3-A-5 Emergency Access Plan

a. **Authority for granting emergency access**: The Immunization Branch Program Manager or his/her designee may declare that an emergency condition exists that requires emergency access to the Registry System. Upon approval by the Registry Coordinator, individuals shall be granted emergency access to the Registry by the Registry System Administrator.
b. **Emergency conditions**: An emergency condition sufficient to allow normal access controls to be bypassed shall be generally accepted to be a situation or set of conditions which satisfy at least one of the following:
    1. A disaster or other situation has rendered Registry access controls inoperative.
    2. A disaster or other situation has rendered the Registry System unable to support business requirements for longer than normal downtime procedures would allow.
    3. A disaster or other situation where Registry staff are required to function beyond their normal defined roles, require immediate access to information beyond their normal access privileges, and the time necessary to alter the access rights of all affected staff members exceed the amount of time that normal downtime procedures would allow.
c. **Contingency Operation Plan**: The Contingency Operation Plan shall contain procedures for emergency access to the Registry System if access becomes unavailable due to an emergency condition.
d. **Temporary nature of emergency access**: All emergency conditions are presumed to be temporary, and access controls are presumed to be suspended for only limited times.

3-A-6 Audit Controls

a. The Registry System shall be configured to produce, store, and retain audit records of specific system, requisite application software, network, and user activity and shall have sufficient storage capacity and defined maximum capacity limitations for audit records. Audit control activities shall include:

1. Identification of events that have occurred, when the events occurred, the source of the events, the cause of the events, and the event outcomes
2. The ability to generate audit record reports for a pre-defined set of events that are adequate to support investigations of security incidents
3. Audit record reports shall include time reports were generated
4. Confidential information shall not be listed in error logs or associated administrative messages

b. **Review of audit records**: The Registry System Administrator or designee shall review Registry System-produced audit records upon request.

3-B Integrity

3-B-1 The Registry System shall be configured to protect the integrity of the data from improper alteration or destruction by restricting permissions according to the user's assigned level of access. Additional tools, including those used to protect against malicious software, shall be identified and utilized to ensure Registry System integrity.

3-B-2 Person or Entity Authentication

a. Authorized users shall be required to log in to the Registry using an assigned user name and a unique password. After a specified number of unsuccessful log in attempts, the system shall lock out the person attempting to gain access to the Registry System until an authorized Registry technical support staff unlocks the account and resets the password.
b. Authorized users shall not have access to the Registry from more than one workstation simultaneously.
c. Exception: The Registry System Administrator and/or designee shall be exempt from item 3-B-2-b (above) when simultaneous access is needed during the course of his/her duties.

3-C Transmission Security

3-C-1 The Registry System shall be configured to prevent unauthorized access and modification of information as it is transmitted over an electronic communications network (e.g. Internet).

a. Registry information shall be encrypted when electronically transmitted, copied, or transferred.
b. All traffic between the web server and client browsers shall be encrypted (minimum 128-bit encryption level).
c. The Registry System shall encrypt data prior to sending through a secure (HTTPS) data transport.
d. The Registry System shall be configured to ensure secure real time data exchanges.
e. The Registry System shall comply with HDOH infrastructure guidelines to protect external and internal infrastructures (i.e. firewalls, DMZ, other). The designated alternate processing sites shall provide the same level of protection.
f. Any connection to the Registry System shall occur through controlled interfaces.
g. Network connections shall be properly terminated at the end of user sessions.
h. Network connections shall be terminated automatically upon a specified period of inactivity or other identified events.
i. Intrusion tools and techniques shall be utilized to provide real-time identification of any unauthorized use, misuse, and abuse of the Registry System.

4. Policies and Procedures

The Registry Security Policy shall govern the administrative, physical, and technical safeguards of the Registry System. The Registry System Administrator and/or designated personnel are responsible for overseeing the development, approval, implementation, and management of the Registry Security Policy and any procedures developed to implement the Registry Security Policy.

4-A Documentation

4-A-1 The Registry Security Policy and any procedures developed to implement the Registry Security Policy shall be documented and maintained in accordance with the following:

a. **Time Limit:** All documentation shall be maintained for a period of six (6) years from date of creation or the date when it was last in effect, whichever is later and in accordance with the official record retention schedule assigned by the Department of Accounting and General Services (DAGS) Archives Division, Records Management Branch.

b. **Availability:** The Registry Security Policy shall be distributed to all authorized users and those who may have a need to know, and supporting documentation shall be available upon request.

c. **Updates:** The Registry Security Policy shall be reviewed and updated by the Immunization Branch at least annually or in response to any significant change that may affect Registry System security.

Glossary

Access
The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any Registry System resource.

Account
User parameters assigned to identify, authenticate, and authorize access to the Registry, minimally comprised of a unique username and password; authentication does not automatically imply authorization.

Administrative Safeguards
Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect individually identifiable health information (IIHI) included in the Registry and to manage the conduct of authorized users in relation to the protection of that information.

Archive
The process of moving records from the Registry System to a separate location for permanent or long-term preservation.

Audit Logs
A chronological record of system activities which documents a sequence of events for examination, used for maintaining security and recovering lost transactions or information and monitoring use of the Registry System.

Audit Records
Documentation of persons accessing the Registry System and operations performed.

Authorized User
Those individuals and/or entities that require access to client immunization and other Registry information for authorized purposes and/or to maintain the Registry system,

Authorized Purposes

Authorized purposes for Registry access include:

a. Consolidating, maintaining, and accessing computerized immunization records;
b. Consolidating and maintaining vaccine inventory information;
c. Determining the immunization history of a client and delivering health care treatment accordingly;
d. Generating notices for clients who are due or overdue for immunizations and in the event of a vaccine recall;
e. Staying abreast of the complex immunization schedule by utilizing registry-supplied immunization forecasting algorithms;
f. Assessing the immunization rate of their client population (or subsets thereof);
g. Generating immunization records (e.g. Student's Health Record);
h. Ensuring compliance with mandatory immunization requirements;
i. Recording the distribution of prophylactic and treatment medications administered or dispensed in preparation for and in response to a potentially catastrophic disease threat; and
j. Other purposes determined at the discretion of the Immunization Branch.

Immunization Branch-specific authorized purposes for Registry access include:

a. Ensuring compliance with mandatory immunization requirements;
b. Performing Quality Improvement/Quality Assessment activities;
c. Complying with Hawaii Vaccines For Children Program vaccine accountability policies and procedures;
d. Preventing and managing outbreaks of vaccine-preventable diseases and other public health emergencies;
e. Producing immunization assessment reports to aid in the development of policies and strategies to improve public health;
f. Managing and maintaining the Hawaii State Immunization system; and
g. Other purposes determined at the discretion of the Immunization Branch.

Availability
The property that Registry System data or information is accessible and useable upon demand by an authorized person.

Confidentiality
The property that data or information is not made available or disclosed to unauthorized persons or processes.

Controlled Interfaces (referenced in Transmission Security)
Devices or interfaces that are inventoried, implemented, and managed by the System Administrator.

Corrective Action Plan
Plan used to identify and assign responsibilities for measures and activities necessary to decrease risk to an acceptable level with minimal adverse impact.

Data Backup Plan
Policies and procedures to create and maintain retrievable exact copies of electronic data and related technology components that are necessary for recovery activities of data so that these additional copies may be used to restore the original after a data loss event.

Disaster Recovery
The process, policies and procedures of restoring operations critical to the resumption of business, including regaining access to data (records, hardware, software, etc.), communications, workspace, and other business processes after a natural or human-induced disaster.

Disclosure
The release, transfer or provision of; access to; or divulgence in any other manner of a client's individually identifiable health information to parties outside the Registry and/or its authorized users.

DMZ (Demilitarized Zone)
A network or computer host that serves as a neutral zone between an internal network (Hawaii Department of Health) and the external network (Internet), allowing services to the external network while preventing unauthorized access to the internal network.

Equipment
Any computer hardware or software or machinery connected to or operated by means of a micro or data processor chip.

Encryption
Translation of data into a form in which there is a low probability of assigning meaning without use of a confidential process or key, helping to protect information from unauthorized viewing or use, especially during transmission or when stored on transportable media.

Firewall
A system that helps protect computers and computer networks from attack and subsequent intrusion by restricting the network traffic which can pass through them and denying access to unauthorized users, based on a set of rules defined by the/a system administrator.

Individually Identifiable Health Information (IIHI)
Information, including demographic and immunization record data, as well as other information that relates to the provision of immunizations to the client.

Integrity
The property that data or information have not been altered or destroyed in an unauthorized manner.

Interface
A boundary across which two independent systems meet and act on or communicate with each other.

1. User interface - the keyboard, mouse, menus of a computer system. The user interface allows the user to communicate with the operating system.
2. Software interface - the languages and codes that the applications use to communicate with each other and with the hardware.
3. Hardware interface - the wires, plugs and sockets that hardware devices use to communicate with each other.

Levels of Sensitivity
Classification levels assigned to data elements, corresponding to the potential impact affecting the privacy of an individual if inappropriately disclosed.

Log In
Process of authenticating the identity of a user attempting to access the Registry System, requiring the user to enter a correct user name and password combination.

Malicious Software (or Malware)
Software or embedded code intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of the Registry System; includes computer viruses, worms, trojan horses, spyware, adware, and other malicious and unwanted code.

Media Destruction and Disposal
The process of destroying and disposing of storage devices or electronic media that contain Registry information.

Permission
Access rights that control the ability of authorized users to view or make changes to the Registry System.

Registry Operations Centers
Facilities in which the Registry System is physically located.

Registry System
The Registry application, hardware, infrastructure, third party software, and data.

Registry System Administrator
The individual identified by the Immunization Branch and assigned the responsibility of maintaining and operating the Registry System.

Sanitization
The process of permanently removing Registry information from a storage device or electronic medium, so that it may be re-used.

Screensaver
A computer program designed to conserve the image quality of computer displays by blanking the screen or filling it with moving images or patterns when the computer is not in use.

Secure (HTTPS) Data Transport
Network protocol for establishing secure connections for exchanging information on the Internet, ensuring reasonable protection from disclosure to unauthorized individuals.

Security
The condition that prevents unauthorized persons from having access to the Registry System, and the policies and procedures that encompass the administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of the Registry System.

Security Incident
The attempted or successful unauthorized access, use, disclosure, modification, or destruction of the information in the Registry System, or interference with Registry System operations.

Significant Change
A physical, administrative, or technical modification to the Registry System or its operations that could affect the confidentiality, integrity, security, or availability of the Registry System.

Social Engineering
Techniques used to manipulate people to perform actions or divulge confidential information in an unauthorized manner.

Storage Equipment
Hardware that stores electronic information, including but not limited to, hard drives, floppy diskettes, CD/DVDs, sim cards, thumb or USB drives, optical disks, magnetic tapes, and zip drives.

System Failover
A backup operation that automatically and transparently to the user redirects requests from the failed or down primary system to the backup system if the primary system fails or is temporarily shut down for servicing. The backup system will mimic the operations of the primary system.

User Access
Security levels assigned to authorized users, corresponding to the user's role and need to access and modify data.

Workstation
An electronic computing device, connected to the Network or "stand alone," for example, a laptop or desktop computer, with a monitor, keyboard, and mouse, or any other device that performs similar functions, and electronic media stored in its immediate environment.