



Iowa's Immunization Registry Information System (IRIS) Security and Confidentiality Policy January 2017

I. Background

IRIS is a statewide immunization and health screening information system managed by the Iowa Department of Public Health's Immunization Program. IRIS was developed to achieve complete and timely immunization of all Iowans. A barrier to reaching this goal is the continuing difficulty of keeping immunization records accurate and up-to-date. IRIS addresses this problem by collecting immunization information from public and private health care providers and linking individual immunization records. When an individual receives immunizations from more than one health care provider, IRIS merges the immunization information from all sources to create a comprehensive record. This assists health care providers in identifying which immunizations are needed for individuals in their care regardless of where they received previous vaccines.

II. Statement of purpose

IRIS is an immunization and health screening information system that serves the public health goal of preventing and mitigating the spread of vaccine-preventable diseases in Iowa. IRIS accomplishes this goal through providing accurate and timely immunization information for all Iowans to assist health care providers in offering age-appropriate immunizations to their patients.

The success and effectiveness of IRIS in achieving its public health goal is dependent on the level of participation by health care providers.

Under Iowa Administrative Code 641-7.11(22); the purposes of IRIS are as follows:

- maintain a database of immunization histories and health screening information
- ensure patients are fully immunized and screened

III. Purpose of security and confidentiality policy

The purpose of this policy is to address the need to provide appropriate security and confidentiality protection to the information in IRIS. The confidentiality of this information must be distinguished from issues of privacy. Privacy is concerned with the control individuals exert over the release of their personal information. Under this policy, confidentiality is concerned with how the information provided to IRIS by individuals is accessed, collected, stored, used, and provided to other individuals and organizations. In addition, security addresses the physical and other measures taken to guard against attack or breach of this information.

IV. Definitions

- A. All terms used in this policy have the same meaning as those terms used in the state law and administrative rules that authorize IRIS.
- B. “Enrolled User” means a user of the registry who has completed an enrollment form that specifies the conditions under which the registry can be accessed and who has been issued an identification code and password by the Iowa Department of Public Health.
- C. “Confidentiality” means
 - 1. limiting the collection, access, use, storage, and release of information from enrolled users to IRIS and from IRIS to enrolled users in a manner that information will not be shared with non-enrolled users, and
 - 2. information will only be used for the purposes permitted under the applicable laws, rules, and policies.
- D. “Department” means the Iowa Department of Public Health.
- E. “Immunization Record” includes, but is not limited to:
 - 1. Name of patient;
 - 2. Gender of patient;
 - 3. Date of birth;
 - 4. Race;
 - 5. Ethnicity;
 - 6. Birth state and birth country;
 - 7. Address;
 - 8. Parents’ names;
 - 9. Mother’s maiden name;
 - 10. Type of vaccination administered;
 - 11. Dose or series number of vaccine;
 - 12. Date vaccination was administered;
 - 13. Lot number;
 - 14. Provider name, license, and business address; and
 - 15. Patient history, including previously unreported doses.
- F. “Health Screening Record” includes a vision screen, dental screen, or refugee health screen.
- G. “Immunization tracking and recall record” includes but is not limited to:
 - 1. Name of patient;
 - 2. Date of birth;
 - 3. Parent/Guardian;
 - 4. Address of the patient;
 - 5. Telephone number;
 - 6. Vaccines needed for the purposes of informing the patient, parent or guardian that the patient is due or past due to receive the recommended immunizations.
- H. “Security” means physical and other measures taken to guard against attack or breach.

V. Confidentiality

Based on the Iowa law (Iowa Code § 22.7(2) and 641 IAC Chapter 7), rules, and general principles of confidentiality, the security and confidentiality policy for IRIS is as follows:

- A. Information in IRIS is confidential under Iowa law. Enrolled users shall not release immunization or health screening data obtained from the registry except to the person immunized or screened, the parent or legal guardian of the person immunized or screened, admitting officials of licensed child care centers and schools, medical or health care providers providing continuity of care, and other enrolled users of the registry.
- B. Immunization and health screening information, including identifying and demographic data maintained in the registry, is confidential and may not be disclosed except under the following limited circumstances:
 1. The Department may release information from IRIS to the following:
 - a) The person immunized or screened, the parent or legal guardian of the person immunized or screened;
 - b) Enrolled users of the registry who have completed an enrollment form that specifies the conditions under which the registry can be accessed and who have been issued an identification code and password by the department;
 - c) Persons or entities requesting immunization or health screening data in an aggregate form that does not identify an individual either directly or indirectly.
 - d) Agencies that complete an agreement with the department which specifies conditions for access to registry data and how that data will be used. Agencies shall not use information obtained from the registry to market services to patients or non-patients, to assist in bill collection services, or to locate or identify patients or non-patients for any purposes other than those expressly provided in this policy.
 - e) A representative of a state or federal agency, or entity bound by that state or federal agency, to the extent that the information is necessary to perform a legally authorized function of that agency or the department. The state or federal agency is subject to confidentiality regulations that are the same as or more stringent than those in the state of Iowa. State or federal agencies shall not use information obtained from the registry to market services to patients or non-patients, to assist in bill collection services, or to locate or identify patients or non-patients for any purposes other than those expressly provided in this rule.
 - f) The admitting official of a licensed child care center, elementary school, or secondary school; or medical or health care providers providing continuity of care.
 - g) Enrolled users from other states or jurisdictions who have signed and completed enrollment in the state's or jurisdiction's immunization registry.
 2. Enrolled users
 - a) Only enrolled users of IRIS may provide information to or receive information from IRIS.
 - b) Information from the immunization or health screening record may only be accessed and shared to perform a legally authorized function of the enrolled users as follows:
 - 1) with other enrolled users
 - 2) with the patient's health care provider and another clinician
 - 3) with a school the patient attends
 - 4) with a licensed child care center the patient attends

- c) Information from the immunization tracking and recall record may only be used by enrolled users to contact individuals (or parents of minor children) for the purposes of informing the individual (or parent or guardian) that he/she is due or past due to receive recommended immunizations. This information may be accessible for entry and updates via the IRIS user interface for health care providers and their staff to ensure accurate data captures. However, access to and use of this information is restricted to the purposes outlined in this policy. Information from the immunization and tracking record will not appear on any reports outside of reminder/recall.
- d) All enrolled users are required to complete an Individual User Agreement and to read and abide by this security and confidentiality policy.
- e) All enrolled users may receive information from IRIS.
- f) Written or verbal permission from the parent or guardian is not required to release information from IRIS.
- g) The IRIS database will maintain an audit trail for all information received from or released from IRIS.
- h) The Department shall seek appropriate penalties for any misuse of information in IRIS by any authorized user or any other party, including pursuing any sanction authorized under state or federal law.
- i) An enrolled user shall shred any paper copy of information from IRIS before disposal.

VI. Security

- A. Access to IRIS is authorized under the conditions required to perform a legally authorized function of the organization.
- B. An enrolled user shall:
 - 1. Review and abide by the IRIS Security and Confidentiality Policy
 - 2. Renew the security certification within IRIS annually
 - 3. Maintain confidentiality
 - 4. Make a reasonable effort to ensure the accuracy of all immunization and demographic information entered or edited
 - 5. Maintain a unique login to access IRIS. Under no circumstances shall user names and passwords be shared.
 - 6. Make every effort to protect IRIS screens from unauthorized view
 - 7. Assure virus protection is in place for each computer on which IRIS is accessed within the organization
 - 8. Encrypt and send securely all data from IRIS before transmission
 - 9. Not copy confidential data onto personal or removable devices (including, but not limited to, flash drives, portable hard drives, memory cards, DVDs, CDs, cell phones, etc.)
- C. Enrolled users must have physical security and password screen savers for all desktop computers/laptops, which must lock or terminate to protect patient information, in accordance with organizational policies and practices, when the computers are not being used.
- D. IRIS information in a paper copy shall not be left where it is visible for unauthorized personnel and must be shredded before disposal.
- E. Any activity that could jeopardize the proper function and security of IRIS shall not be conducted.
- F. The IRIS Administrative User at each organization must terminate access for an authorized user who no longer requires access.

- G. Violators of this policy will be restricted from IRIS by the IRIS Administrative User at the organization or by the IRIS Coordinator. The Department shall seek appropriate penalties for any misuse of information in IRIS by any enrolled user or any other party, including pursuing any sanction authorized under state and federal law.

VII. Annual review of security and confidentiality among IRIS staff and users

Enrolled health care providers shall annually review this IRIS Security and Confidentiality Policy, the IRIS Security Notification within IRIS, and review the Individual User Agreements/Authorized Site Agreement-Organization form.

VIII. Requests for information

- A. Individuals, parents and guardians may request immunization or health screening data by completing the appropriate IRIS Record Request Form, which is found under the 'Forms' tab of IRIS at <https://iris.iowa.gov>.
- B. All subpoenas, requests for production, warrants, and court orders will immediately be referred to the Office of the Attorney General.

IX. Data retention and disposal

IRIS is in compliance with the State Records Commission as all data is entered and maintained in electronic form for the life of the registry. Monthly, the full IRIS database is backed up and archived to tape. Monthly archive backups are maintained for one year.

X. Voluntary Opt-Out

In any circumstance in which a parent or guardian specifically requests the removal of information on their child from IRIS or an adult over the age of 18 requests their information be removed, the record will be removed. Patients, parents and guardians requesting voluntary opt-out must also notify their health care provider(s) to prevent creation of additional records in IRIS, either via electronic submission from an electronic health record system or direct entry in IRIS. Requests to remove records must be in writing, and must be sent to the attention of the IRIS Coordinator.

IRIS Coordinator
Iowa Department of Public Health
Immunization Program
321 East 12th Street
Des Moines, IA 50319-0075

XI. Prohibited Transfer of Data or Secondary Use of IRIS data

Enrolled users are not permitted to transfer data, either in paper or electronic form, to non-enrolled users. Non-enrolled users include, but are not limited to, software vendors, contractors, and quality improvement organizations. Enrolled users may share IRIS data with these entities only when performing legally authorized functions of the enrolled user.

XII. Use of IRIS data

The registry shall contain immunization and health screening information, including identifying and demographic data, to allow enrolled users to maintain and access a database of immunization and health screening histories for purposes of ensuring that patients are fully immunized and screened. The registry may be used to track inventory or utilization of pharmaceutical agents identified by the Department to prepare for or respond to an emergency event. Enrolled users shall not use information obtained from the registry to market services to patients or nonpatients, to assist in bill collection services, or to locate or identify patients or nonpatients for any purpose

other than those expressly provided in this rule. The registry shall contain health screening data, including screening results and follow-up information.

Any request for information from IRIS that does not satisfy the above criteria may only be provided to the requestor in aggregate form that does not identify an individual. Notwithstanding the above, the Department may consider other requests for research.

XIII. Penalties

The Department shall seek appropriate penalties for any misuse of information in IRIS by any enrolled user or any other party, including pursuing any sanction authorized under state and federal law.