



## Iowa Department of Public Health Immunization Registry Information System (IRIS) Security and Confidentiality Policy October 2021

### 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. IRIS combines immunization data and health screening records from multiple health care providers and merges the information from all sources to create a comprehensive record. This assists health care providers in identifying which immunizations and health screenings are needed for individuals regardless of where services were provided. Contact the IRIS Help Desk at 800-374-3958 with questions about IRIS or this policy.

### Purpose of IRIS

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 and assuring individuals receive proper health screenings.

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

### Purpose of the Security and Confidentiality Policy

The purpose of this policy is to address the need to provide appropriate security and confidentiality protection for 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 personal identifiable information. Under this policy, confidentiality is concerned with how the information provided to IRIS by individuals is accessed, collected, stored, used, and provided to individuals and organizations. In addition, security addresses the physical and other measures taken to guard against attack or breach of this information.

## **Permitted Use of IRIS**

The permitted use of IRIS is to ensure patients are fully immunized with all recommended vaccines and have received appropriate health screenings consistent with Iowa Administrative Code. The purpose and permitted use of IRIS is in accordance with 641 Iowa Administrative Code 7.11(2).

Iowa state law [Iowa Code § 22.7(2) and 641 IAC Chapter 7] specifies immunization and health screening information is confidential, and may only be shared with enrolled users, an individual's health care provider, school, child care facility, local health department, the individuals themselves or parent/guardian if the person is a minor.

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 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.

Health care providers may use IRIS to view patient immunization records for other medical procedures with the intent of ensuring patients are age-appropriately immunized or screened. For example, a health care provider may use IRIS to view a patient's immunization record prior to an upcoming surgery to ensure the patient is appropriately immunized or screened; if the patient is not appropriately immunized or screened, the provider must offer any missing immunizations or screenings or provide referral information for such services.

Generally, employers cannot enroll to use IRIS solely to verify employee vaccination status. Employers can obtain vaccination status directly from the employee. However, enrolled users within health care facilities may use IRIS to view and maintain a record of immunizations received for the purpose of ensuring employees are appropriately immunized to prevent the spread of vaccine-preventable diseases among patients served. Health care facilities are defined as an institution providing health care services or a health care setting including, but not limited to, hospitals, nursing facilities, and assisted living programs. If the employee is not appropriately immunized, the employer must offer any missing immunizations or screenings or provide referral information for such services.

Use of IRIS for purposes other than as described above and in any other manner which is inconsistent with 641 Iowa Administrative Code 7.11(2) is not permitted. Unauthorized use of IRIS is prohibited by law and may result in suspension or termination of user access as well as criminal and civil penalties (Iowa Code sections 135.38 and 139A.25, 641 IAC 7.11, 641 IAC 175.13(2)(a)(8)).

## Definitions

All terms used in this policy have the same meaning as those terms used in the state law and administrative rules that authorize IRIS.

- A. "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.
- B. "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.
- C. "Department" means the Iowa Department of Public Health.
- D. "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.
- E. "Health Screening Record" includes a vision screen, dental screen, or refugee health screen.
- F. "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.
- G. "Security" means physical and other measures taken to guard against attack or breach.

## 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) Written or verbal permission from the parent or guardian is not required to release information from IRIS if releasing to anyone in the following list. 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 or guardians 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 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) The IRIS database will maintain an audit trail for all information received from or released from IRIS.
- g) 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 or federal law.
- h) An enrolled user shall shred any paper copy of information from IRIS before disposal.

## **Security**

Security addresses the physical and other measures taken to guard against attack or breach of IRIS information.

- 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. Enter data timely and accurately, and not knowingly enter invalid/false data, falsify any document or data obtained from IRIS
  6. Maintain a unique login to access IRIS. Under no circumstances shall usernames and passwords be shared
  7. Make every effort to protect IRIS screens from unauthorized view
  8. Assure virus protection is in place for each computer on which IRIS is accessed within the organization
  9. Encrypt and send securely all data from IRIS before transmission
  10. 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. IRIS must only be accessed using an approved work device for the organization which completed the IRIS enrollment. IRIS users shall not access IRIS using a personal computer or other personal devices.
  - D. Enrolled users must have physical security and password screensavers 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.
  - E. IRIS information in a paper copy shall not be left where it is visible for unauthorized personnel and must be shredded before disposal.
  - F. Any activity that could jeopardize the proper function and security of IRIS shall not be conducted.
  - G. The IRIS Administrative User at each organization must terminate access for an authorized user who no longer requires access.
  - H. 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. Unauthorized use of this system is prohibited by law and may result in criminal and civil penalties (Iowa Code sections 135.38 and 139A.25, 641 IAC 7.11(4), 641 IAC 175.13(2)(a)(8)).

### **Annual Review of Security and Confidentiality Policy**

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.

### **Release of IRIS Information**

IRIS records are confidential and may only be released to the following individuals authorized by law:

1. A parent or legal guardian.

2. A legal guardian for a ward (protected person) regardless of the age of the ward.
3. Individuals over the age of 18.

Requests for IRIS records may not be accepted for a spouse, partner, child over the age of 18, or employee. Individuals, parents and guardians may request immunization or health screening data by completing the IRIS Record Request Form, which is found under the 'Forms' tab of IRIS at <https://iris.iowa.gov>. The Record Request Form and a copy of a state-issued ID (such as Driver's License) shall be emailed to [irisenrollment@idph.iowa.gov](mailto:irisenrollment@idph.iowa.gov). By signing the IRIS Record Request form, the requester declares under penalty of perjury under the laws of the State of Iowa that she/he is the subject of the record or the parent or legal guardian of the subject of the record and are therefore authorized to access the record. By completing this record request form, the requester verifies the information is true and accurate, and the requester is authorized by law to have the record. All subpoenas, requests for production, warrants, and court orders will immediately be referred to the Office of the Attorney General. Unauthorized use of IRIS is prohibited by law and may result in criminal and civil penalties (Iowa Code sections 135.38 and 139A.25, 641 IAC 7.11(4), 641 IAC 175.13(2)(a)(8)).

## **IRIS and HIPAA**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) governs the use and disclosure of protected health information. It applies to:

- Health plans and providers ("covered entities")
- Business associates of who perform legal, accounting or other services for covered entities

HIPAA Section 164.512(b) permits a covered entity to disclose protected health information for public health activities.

### **Impact of HIPAA on Immunization Information Systems (IIS):**

HIPAA does not limit IIS activities because the Privacy Rule permits disclosure to public health authorities and their authorized agents for public health purposes.

- Public health authorities operate IRIS in Iowa.
- Iowa state law allows the sharing of IRIS information with enrolled users. [Iowa Code § 22.7(2) and 641IAC Chapter 7]

### **Impact of HIPAA on clinic and health plan release of immunization data to IRIS:**

Enrolled users can submit electronic, hard copy, or web entered immunization data to IRIS. Covered entities (providers, clinics, health plans, etc.) may disclose protected health information to IRIS without having to obtain advance permission from patients according to HIPAA Section 164.512(b). IRIS can re-disclose immunization information to enrolled users in accordance with Iowa state law [641IAC Chapter 7].

### **Impact of HIPAA on accounting for public health disclosures:**

A simplified accounting for Public Health purposes may be used if during the accounting period the covered entity made multiple disclosures to the same recipient for the same



purpose. In such cases, the covered entity need only identify the recipient [IRIS] of such repetitive disclosures, the purpose of the disclosure, and describe the protected health information [immunization records] routinely disclosed. The date of each disclosure need not be tracked. The covered entity would not need to annotate each patient's medical record whenever a routine public health disclosure was made (MMWR April 11, 2003/52; Pg.9).

### **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.

Audit tables within the IRIS database are maintained for a period of 5 years. Audit tables may include but are not limited to patient searches, reminder/recall reports, user names, inventory reports, and ad hoc reports.

### **Participation in IRIS**

Enrolled users can submit electronic, hard copy, or web entered immunization data to IRIS. Covered entities (providers, clinics, health plans, etc.) may disclose protected health information to IRIS without having to obtain advance permission from patients according to HIPAA Section 164.512(b). In circumstances in which a parent or guardian specifically requests the removal of information for 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, either by mail or email, and must include the name and date of birth of the person whose record should be removed. Requests must be sent to the attention of the IRIS Coordinator. If sent by email, the subject line should be titled 'IRIS Opt Out Request'.

IRIS Coordinator  
Iowa Department of Public Health  
Immunization Program  
321 East 12<sup>th</sup> Street  
Des Moines, IA 50319-0075  
[irisenrollment@idph.iowa.gov](mailto:irisenrollment@idph.iowa.gov)

### **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.



## **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. The Department may suspend or terminate an enrolled user's access consistent with Department policy if the user violates this Iowa Administrative Code Chapter 7, the IRIS Authorized Site Agreement-Organization, the IRIS Authorized Individual User Agreement, or the IRIS Security and Confidentiality Policy. The Department shall approve, suspend, terminate, and reinstate user access in accordance with Iowa Administrative Code Chapter 7 and Department policy. Unauthorized use of IRIS is prohibited by law and may result in criminal and civil penalties (Iowa Code sections 135.38 and 139A.25, 641 IAC 7.11(4), 641 IAC 175.13(2)(a)(8)).