Immunization Registry Certification

Recommendation of the National Immunization Program's Technical Working Group (TWG)

June 4, 2002

Introduction to Certification

This document has been developed for the purpose of immunization registry certification of minimum functional standards. To become certified, registries must meet all criteria for the minimum functional standards. Certification is a voluntary process, which will be performed at the request of registries according to their self-determination of readiness. Certification is not evaluation. Certification assesses attainment; evaluation measures progress.

The minimum functional standards and criteria for their assessment may become the basis for a registry evaluation. Evaluation would be distinguished from certification by the inclusion of incremental weighted scoring to accurately reflect and encourage registry development. Registry evaluation by the National Immunization Program (NIP) is intended on an annual basis for federally funded immunization grantees.

Organization to Certify Immunization Registries

To date, there has been no success in identifying an outside organization to certify immunization registries due to lack of interest by the organizations approached and no identifiable source of funding.

The TWG recommends establishing a certifying body – **Immunization Registry Certification Commission (IRCC)**. The IRCC will be composed of representatives from organizations that support the certification process. The initial membership of the IRCC will be the current TWG members. Other members may be added if the IRCC members determine that additional representation is necessary to carry out the functions of the group. The IRCC will not be a part of CDC, but will have CDC participation and will use the data collected by NIP in the ongoing annual evaluation process of its grantees.

The IRCC may be established as a 501(3)(C).

Initially, the IRCC will not require funding because it is anticipated that only a small number of registries will request certification in the first 1-2 years. By using the NIP site visit data that is currently collected, the only resources needed would be staff time to put together the data and write up the recommendation. Members of the IRCC will volunteer their time to review the data and decide whether to certify.

Certification Process

- NIP will contract with an outside organization to collect certification information.
- Registries that request certification will agree (by signature on the application for certification) to abide by the decision of the IRCC.
- NIP will receive information collected by the contractor and will provide support staff for the IRCC process.
- The IRCC should expect to receive a well-reviewed application and should not have to communicate back and forth to get the information it needs. However, if the IRCC identifies any deficiencies or incomplete information in the application for certification, it will identify the deficiency and return the application for certification to the data collector to correct and return to the IRCC.
- The IRCC will review the data and analysis provided, make a recommendation to certify or not, and provide written feedback about the registries strengths and weaknesses.
- The IRCC will either certify the registry or reject the application with an explanation of the deficiencies. The written report will reference each standard, describe whether it was met and, if not, what is need by the registry to meet the standard and describe areas that are exceptional or problematic.
- A registry should be recertified every 3 years. A certification expiration date will be assigned when a registry receives notice that they are certified. The expiration date will be 3 years from the date that certification is issued.
- The IRCC will have an appeals process in place for registries that dispute the initial assessment.

Certifying the Immunization Registry Minimum Functional Standards

Note: *These standards only apply to records available in a population-based immunization registry (one that is designed to contain all children in the catchment area) that is operating in compliance with state/local laws and/or policies. For example, in a state where explicit consent is required by law or policy, these standards only apply to records where explicit consent has been obtained.*

Standard #1

Electronically store data on all NVAC-approved core data elements

Definition The registry's computer database contains fields for all NVAC-approved core data elements. These elements are: patient name (first, middle, and last); patient birth date; patient sex; patient birth state/country; mother's name (first, middle, last, and maiden); vaccine type; vaccine manufacturer; vaccination date; and vaccine lot number.

Note: *The core data elements comprise the basic set of data that registries will exchange with each other. They are designed to standardize a set of patient demographic and vaccine event elements that are considered core to record exchange between registries. The mother's name element refers to current legal mother (who may or may not be birth mother). To receive credit for the patient and mother names, at least a surname and one other name element must be valued.*

To meet this standard: All required fields must be present in the database, and each required field must have at least 25% completeness, not including codes for "unknown" or "filler" data (non-relevant data entered to force the computer past a required field).

Preferred method for certifying function: Review a sample of 100% of the registry database for the cohort of children born during the 3-month period ending 8 months prior to the site visit. Historical data[1] may be excluded. Generate a frequency distribution to confirm that at least 25% of each required field is valued. Review the required fields in the database to ensure that entries do not contain codes for "unknown" or "filler" data (non-relevant data entered to force the computer past a required field).

If it is not possible for the registry to generate a frequency distribution, the alternate method below may be used.

Alternate method for certifying function: Each reviewer will be provided with a list from the registry database of all individual clients (identified by a local code identifier only) born during the 3-month period ending 8 months prior to the site visit. From this list, the reviewer will select every *n*th entry (vary the *n*) until a total of 40 clients are chosen. The reviewer will complete a worksheet with space for 40 records, identifying valuation of each required field by the numeral one (1), and absence of valuation, "unknown" or "filler" data as a zero (0). The sum of all entries for each record will be divided by the number of required fields - all must be valued to reach a result of one (1) for that client record. Once ten records are identified with a total score of one (1), no further record review for this standard is required. If all 40 records are reviewed and 10 have not been identified with a score of one (1), the registry receives 0 points for this standard.

Data required for review:

- Database report
- Frequency distribution of required fields

[1] Historical data: Immunizations given prior to the implementation date of the registry, or immunization data captured from a secondary data source (i.e., data reported from a source other than the current immunization provider).

Standard #2

Establish a registry record within *6 weeks* of birth for each newborn child born in the catchment area
Definition Identifying information from a population-based data set (e.g., vital statistics) is regularly sent to or retrieved by the registry in a computer file format that requires little, if any, manipulation by registry staff for the data to be entered into the immunization registry. Such information is available in the registry within 6 weeks of birth.

To meet this standard: 90% of the records must be submitted and registry records established within 6 weeks of birth.

Method for certifying function: Review a sample of 100% of the registry database for the cohort of children born during the 3-month period ending 8 months prior to the site visit. Generate a report showing the difference between the birth date and the registry entry date and calculate the percentage of these records that were established within 6 weeks of birth. *(Note: An alternative method to calculate this percentage may be proposed by the registry and accepted by the reviewers.)*

Data required for review:

- Database report
- Frequency report

Standard #3

Enable access to and retrieval of immunization information in the registry at the time of encounter
Definition The registry provides a means by which providers can access and retrieve immunization records prior to or at the time of a scheduled encounter.[2]
Note: This standard accommodates registries that do not operate continuously (e.g., closed Sundays and holidays) and those that send and receive non-electronic records in order to allow access to users without electronic capabilities. For example, providers can request and receive the immunization record(s) needed from the registry prior to the scheduled encounter (can include printed patient lists, flags on charts, fax or phone requests).

To meet this standard: The registry should enable access to immunization information in the registry prior to or at the time of a scheduled encounter 90% of the time.

Method for certifying function: Reviewers will select 10 records from the sample requested under Standard #2, and then ask the registry to access and retrieve immunization records. Reviewers will observe and document the method of information retrieval. The access methods may include electronic, phone, fax, etc. The reviewer will document the proportion of patients successfully retrieved.

Data required for review:

- A sub-sample of patients drawn from Standard #2
- Screen report(s) for those registries with electronic access
- Copies of forms used for other methods of access

[2] The standard as currently defined will serve as the interim minimum during the initial phase of registry certification; however, the standard will change in 2005 to: “Electronically access immunization information in the registry at the time of encounter.”

Standard #4

Receive and process immunization information within *1 month*[3] of vaccine administration

Definition The registry receives and processes immunization information within 1 month of vaccine(s) administration (e.g., can include fax or phone requests). This will serve as the interim minimum during the initial phase of registry assessment; however, the ideal standard will become the minimum in 2005.[4]

To meet this standard: The registry should receive and process 90% or more of the primary[5] immunization information within 1 month of vaccine administration.

Method for certifying function: Review all of the immunization records in the database for the 3-month period ending 8 months prior to the site visit. The registry will provide the report calculating the percentage of records that were processed within 1 month of vaccine administration.

Data required for review:

- Calculation report

Standard #5

Protect the confidentiality of health care information

Definition The registry has written confidentiality policies and procedures in place and implemented, including administrative and technical practices to protect health care information.[6] The policies and procedures are consistent with applicable state and local laws, Federal law (HIPAA or other privacy law) when implemented, and with the recommended specifications and guidelines outlined in the updated *"Community Immunization Registries Manual: Chapter II: Confidentiality,"* except where they conflict with applicable legislation.

For certification, a registry's **process** for implementing their privacy policy will be evaluated. A Confidentiality Working Group (CWG), to be formed by NIP, will evaluate the **content** of the privacy policy.

To meet this standard:

1. The registry must have the recommendation of CDC's CWG to certify based on the content of the registry's policy to protect privacy and confidentiality.
2. After the registry receives the CWG recommendation to certify, the standard will be evaluated based on the process in place to implement the specifications as described below.

Confidentiality Policies

- The registry should have a written confidentiality policy in place.
- The confidentiality policy should be reviewed at least every 3 years by counsel for consistency with state, local, and/or Federal laws.

Method for certifying function: During onsite visit, interview registry staff to determine that the registry has a written confidentiality policy in place, and that the confidentiality policy has been reviewed within the last 3 years by counsel for consistency with state, local, and/or Federal laws.

Data required for review:

- Confidentiality policy
- Date and results of legal review

[3] For the purposes of this calculation, one month equals 30 days.

[4] The standard as currently defined will serve as the interim minimum during the initial phase of registry assessment; however, the standard will change in 2005 to: "Receive and process immunization information on the day of vaccine administration."

[5] Primary immunization information is immunization data reported by the current immunization provider; i.e., historical data should be excluded.

[6]. Health care information in this document refers to patient demographics, as well as medical conditions, care or services related to the health of the patient.

User Agreements and Confidentiality Statements

- The registry should distribute copies of the confidentiality policy to users[7] before they receive access to the registry.
- The registry should have all users sign user agreements or confidentiality statements prior to receiving access to the registry.
- The registry should provide training on confidentiality to all authorized users at least annually (e.g., online training, email updates, on-site training sessions).

Method for certifying function: During onsite visit, interview registry staff and confirm at the user visit that confidentiality policies are distributed and that user agreements or confidentiality statements are signed. Review or observe training methods and review the training schedule.

Data required for review:

- Copy of user agreement or confidentiality statement
- Copy of training materials
- Copy of training schedule

Notification

- The registry should provide notification to the personal representative about the existence of the registry.
- The registry should provide notification prior to the submission of immunization information into the registry.
- The registry should provide notification in a language that the personal representative can understand.

Method for certifying function: During onsite visit, interview registry staff and confirm at the user visit if notification about the existence of the registry is provided to personal representatives, if it is provided prior to submission of immunization information into the registry, and if it is provided in a manner that they can understand. Determine if notice is written or verbal.

Data required for review:

- If written, copy of notice
- If verbal, copy of a statement describing what the notice contains
- Copy of alternative methods of giving notice (e.g., non-English)

Choice

- The registry should allow the patient's personal representative[8] to choose whether or not to participate in the registry.
- The registry should allow the patient's personal representative to change this decision at any time.
- The registry should not penalize the patient's personal representative for choosing not to participate in the registry.
- The registry should not share personally identifiable information of those who have chosen not to participate in the registry.
- The registry should document verbal choice about participation in the registry.
- The registry should collect separate signatures for consent or opt out and refusal to vaccinate.

[7] A user in this document refers to an entity who has access to health care information in the registry. Users may include health care providers state and local health departments, managed care organizations, school nurses or clinics, and parents. Under appropriate circumstances, non-health care providers such as child care facilities, schools, colleges, WIC programs, and researchers can be authorized users. Authorized users may also include individuals who provide technical support to the registry.

[8] A patient's personal representative in this document refers to a person who has authority to act on behalf of the patient, whether the patient is an adult, an emancipated minor, or an unemancipated minor if the unemancipated minor consents to the health care service and has not requested that another person be treated as the personal representative.

Method for certifying function: Review data collected during site visit to determine if the above actions were carried out. During the onsite visit, interview registry staff and confirm how they execute the above actions.

Data required for review:

- Copies of consent forms, opt out forms, written notifications, documentation of verbal choice

Use of Immunization Registry Information

- The registry should inform all authorized users and/or the patient's personal representatives of the purposes for which immunization information is collected.
- Immunization information in the registry should not be used for any reason other than that for which it was collected.
- The registry should take steps to insure that information in the registry is not used in a punitive manner.
- The registry should notify and give the opportunity to consent to providers if immunization registry information that identifies the provider is used for quality improvement or external reporting.

Method for certifying function: Review data collected during site visit to determine if the above actions were carried out. During the onsite visit, interview registry staff about how they execute the above actions.

Data required for review:

- Written verification documenting the registry's position on use of immunization registry information

Access to and Disclosure of Registry Information

(Note: The elements below that are marked with an asterisk* may overlap with security measures)

- *The registry should ensure that only authorized users provide information to and receive information from the registry.
- *The registry should ensure that authorized users who provide direct service access only records on children or patients under their care or for whom they share clinical responsibility.
- *The registry should ensure that authorized users who finance and manage care (i.e., managed care organizations) access only records on children or patients that are enrolled in their plan.
- *The registry should ensure that patients' personal representatives have access to their own children's records unless there is substantial evidence that the information in the record (e.g., child's address) could reasonably be expected to cause harm to their child or others.
- *The registry should ensure that a patient's personal representative has an opportunity to request a correction and/or amendment to the child's record.
- *The registry should have a process in place to address requests for information from individuals and organizations that are not authorized users.
- *The registry should notify individuals in a timely manner when there is a request for personally identifiable information from an individual or organization that is not an authorized user. The registry should notify individuals in a timely manner in the event of a breach of confidentiality or security if their child's record was involved.
- *The registry should ensure that registry information that is redisclosed is accompanied by a statement that notifies the recipient of the following:
    - that the information disclosed may be from a confidential record protected by state and federal laws;
    - any further disclosure of the information in an identifiable form may be prohibited without the written, informed consent of the person who is the subject of the information or as permitted by federal or state law; and
    - unauthorized disclosure of the information may result in significant criminal or civil penalties, including imprisonment and monetary damages.

- If a patient's personal representative does not have an opportunity to request a correction and/or amendment to the child's record, the registry should provide written notice of the reasons for denial and the patient's personal representative should be able to appeal a denial.
- The registry should immediately refer all subpoenas, requests for production, warrants, and court orders to legal counsel.

Method for certifying function: Review data collected during site visit to determine if the above actions were carried out. During the onsite visit, interview registry staff and confirm how they execute the above actions.

Data required for review:

- Copies of disclosure and redisclosure statement(s), notifications sent to personal representatives, related documents
- Copy of security policies and procedures enforced

Penalties

- The registry should impose and enforce penalties for the inappropriate use or disclosure of information.
- The registry should not impose penalties for good faith disclosure of immunization information to the registry.

Method for certifying function: Review data collected during site visit to determine if the above actions were carried out. During the onsite visit, interview registry staff and confirm how they execute the above actions.

Data required for review:

- Copies of related documents

Data Retention and Disposal

(This may be covered under the security functional standard)

- The registry should delete or archive information at the end of a designated period of time.
- The registry should store or dispose of forms that contain confidential information.

Method for certifying function: Review data collected during site visit to determine if the above actions were carried out. During the onsite visit, interview registry staff and confirm how they execute the above actions.

Data required for review:

- Retention policy
- Copies of related documents

Standard #6

Ensure the security of health care information

Definition The registry has written security policies and procedures in place and implemented, including administrative and technical practices and physical safeguards to protect health care information. The policies and procedures are consistent with applicable state and local laws and with Federal law when implemented.

Note: Appendix D of the "Community Immunization Registries Manual: Chapter II: Confidentiality" will serve as the current recommended specifications and guidelines;however, HIPAA implementation may result in a change in the minimum specification.

To meet this standard: The registry must assess potential risks and vulnerabilities to the individual health data in its possession and develop, implement, and maintain appropriate security measures that are periodically reviewed and updated. These measures, addressing each of the specifications below, must be documented and kept current.

I. Administrative procedures

Definition – The procedures to guard data integrity, confidentiality, and availability including documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data.

Items to be addressed under this specification are:

- **Security certification.** The registry must conduct a technical evaluation, either internal or external, to assess the extent to which their computer system or network design and implementation meets a pre-specified set of security requirements.
- **Data transfer.** The registry should have a signed agreement with each partner[9] (e.g., researchers) with whom they electronically exchange data agreeing to protect the integrity and confidentiality of the data exchanged.
- **Contingency plan.** The registry should implement a routinely updated plan for responding to a system emergency. This plan may include performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from disaster. The plan should address all of the following features:
    - Applications and data criticality analysis
    - Data backup plan
    - Emergency mode operation plan
    - Procedures for testing and revising written contingency plan
    - Disaster recovery plan:
      The registry should have a written backup and recovery plan that provides for regular incremental and periodic full database backup. Backup media should be stored securely in a separate location. In addition, the registry should have a regularly tested (at least annually) disaster recovery plan.
- **Information access management.** The registry should have documented policies and procedures for granting different levels of access to health care information that addresses all of the following features:
    - Access authorization
    - Access establishment
    - Access modification
- **Personnel security.** The registry should ensure that all personnel who have access to any individually identifiable information have the required authorization as well as all appropriate clearances. The registry should address all of the following features:
    - Assure that operating and maintenance personnel have proper access authorization and supervision
    - Establish personnel clearance procedures
    - Maintain a record of access authorizations
    - Establish and maintain personnel security policy/procedure
    - Assure that system users receive security awareness training
    - Establish termination procedures that include appropriate security measures, e.g.,
        - Change combination locks
        - Remove user from access lists
        - Remove user account(s)
        - Retrieve user keys, token or access cards
- **Assign security responsibility.** The registry should have a practice established to manage and supervise the execution and use of security measures to protect data and manage and supervise the conduct of personnel in relation to the protection of data
- **Security configuration management**. The registry should have measures, practices, and procedures for the security of information systems that can be coordinated and integrated with each other and other measures, practices and procedures of the organization established in order to create a coherent system of security. The registry should address all of the following features:
    - Documentation of security system
    - Review and test hardware/software installation and maintenance for security features
    - Inventory hardware and software assets

[9] Partner in this document refers to the sender or receiver of electronic information to an immunization registry.

    - Conduct/implement security testing
    - Conduct/implement virus checking
- **Security incident procedures.** The registry should implement documented instructions for reporting security breaches that address all of the following features:
    - Report procedures to document security incidents
    - Response procedures to be taken as a result of a security incident report
- **Security management process.** The registry should have a process in place for the creation, administration, and oversight of policies to ensure the prevention, detection, containment, and correction of security breaches involving risk analysis and risk management. This process should address the following features:
    - Risk analysis
    - Risk management
    - Sanction policies and procedures
    - Security policy
    - Regular review of systems activity logs and audit trails
- **Training.** The registry should provide education concerning the vulnerabilities of the health information in the registry's possession and ways to ensure the protection of the information. Training may consist of the following features:
    - Provide awareness training for all personnel (including management)
    - Issue periodic security reminders
    - Educate users concerning virus protection
    - Educate users of importance of monitoring log-in success/failure and how to report discrepancies
    - Educate users about password management

Method for certifying function: Review data collected during the site visit to determine if the above actions were carried out. During the onsite visit, interview registry staff and confirm with users how the above actions are executed.

Data required for review:

- Documentation of administrative procedures

II. Physical safeguards

Definition – The safeguards to guard data integrity, confidentiality, and availability. Physical safeguards protect physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Physical safeguards also cover the use of locks, keys, and administrative measures used to control access to computer systems and facilities.

Items to be addressed under this specification are:

- **Facility access controls (limited access).** The registry should have documented policies and procedures to be followed to limit physical access to an entity while ensuring that properly authorized access is allowed. The registry should address the following features:
    - Facility security plan
    - Procedures for verifying access authorizations prior to physical access
    - Maintenance records
    - Need-to-know procedures for personnel access
    - Sign-in for visitors and escort, if appropriate
    - Testing and revision
- **Policy/guideline on workstation use:** The registry should provide documented instructions/procedures delineating the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific computer terminal site or type of site, dependent upon the sensitivity of the information accessed from that site.
- **Media controls.** The registry should have documented policies and procedures that govern the receipt and removal of hardware/software into and out of a facility. The registry should address the following features:
    - Accountability (tracking mechanism)
    - Data backup
    - Data storage

  - Disposal
  - Media reuse procedures
- **Workstation security:** The registry should provide physical safeguards to eliminate or minimize the possibility of unauthorized access to information.

Method for certifying function: Review data collected during the site visit to determine if the above actions were carried out. During the onsite visit, interview registry staff and confirm how the above actions are executed.

Data required for review:

- Documentation of physical safeguards

III. Technical security services

Definition – The processes to guard data integrity, confidentiality, and availability, including those that are put in place to protect information and to control individual access to information.

Items to be addressed under this specification are:

- **Access control**: The registry should address emergency access and a mechanism to restrict access
- **Audit controls**: The registry should address mechanisms employed to record and examine system activity.
- **Authorization control:** The registry should address a mechanism for obtaining consent for the use and disclosure of health information that may include one of the following implementation features:
  - Role-based access
  - User-based access
- **Data authentication:** The registry should have corroboration that data has not been altered or destroyed in an unauthorized manner (e.g., use of check sum, message authentication code, digital signature)
- **Entity authentication:** The registry should have corroboration that an entity is the one claimed including automatic log off (or equivalent) and unique user identifier. Registries should consider adding at least **one** of the following:
  - Biometric identification
  - Password
  - Personal Identification Number (PIN)
  - Telephone callback procedure
  - Token

Method for certifying function: Review data collected during the site visit to determine if the above actions were carried out. During the onsite visit, interview registry staff and confirm with users how the above actions are executed.

Data required for review:

- Documentation of technical security services

IV. Technical security mechanisms

Definition -- The processes that are put in place to guard against unauthorized access to data that is transmitted over a communications network.

Item to be addressed under this specification is:

- **Transmission security**. If the registry employs network communications, the security standards for technical security mechanisms should address integrity controls and message authentication and must implement encryption if Internet is used as a transmission media.

Method for certifying function: Review data collected during the site visit to determine if the above actions were carried out. During the onsite visit, interview registry staff and confirm how the above actions are executed.

Data required for review:

- Documentation of technical security mechanisms

Standard #7

Exchange immunization records using Health Level Seven (HL7) standards

Definition The registry has a function, at the central level, that creates, receives, and properly processes the HL7 messages, as specified in NIP's Implementation Guide for Immunization Data Transactions using Version 2.3.1 of the Health Level Seven (HL7) Standard Protocol (Guide), June 1999.

To meet this standard: The registry must demonstrate that it can properly create, receive and process the HL7 messages as specified in NIP's Guide.

Method for certifying function: To demonstrate the ability to process messages: registries will establish a test file for receiving records; reviewers will provide a test data set of 40 messages (10 messages of each of the four types) that the registry will process; and the registry will print the results from the test. Reviewers will observe the registry as it processes the data. To demonstrate the ability to create a message, the reviewers will provide a set of immunization records that the registry will use to create the test messages.

Data required for review:

- Documentation of the registry's processing of the HL7 records
- Summary comments verifying whether the registry successfully processed the test cases

Standard #8

Automatically determine the routine childhood immunization(s) needed, in compliance with current ACIP recommendations, when an individual presents for a scheduled immunization

Definition The registry has an automated function, accessible at the provider level, that determines needed routine childhood immunizations, in compliance with current ACIP recommendations, given an individual's immunization history to date.

To meet this standard: The registry must demonstrate that it can determine needed routine childhood immunizations, in compliance with current ACIP recommendations, given an individual's immunization history to date.

Method for certifying function: CDC test cases will be used to certify registry algorithms. Reviewers will discuss results with registry staff to determine reasons for any variance from ACIP recommendations. Even though the standard requires compliance with the ACIP recommendations, reviewers will collect documentation on any differing state requirements to be considered in the certification process.

Data required for review:

- Comparison of registry automated recommendations and ACIP recommendations

Standard #9

Automatically identify individuals due/late for immunization(s) to enable the production of reminder/recall notifications

Definition The registry has an automated function that produces a list of individuals who, as of a given date, are due or late for immunizations according to the registry's algorithm (see Functional Standard #8). The output from this function gives the ability to produce reminder or recall notices.

To meet this standard: The registry must demonstrate that it can produce a list of individuals who, as of a given date, are due or late for immunizations according to the registry's algorithm and can produce reminder or recall notices.

Method for certifying function: Reviewers should ask the registry to demonstrate the reminder/recall function during the site visit based on a subset of test cases (10 or more) used for Standard #8 certification.

Data required for review:

- Results of the processing of subset of test cases used for Standard #8 certification
- Summary comments verifying whether the registry successfully identified individuals due or late for immunizations and generated reminder/recall notices

Standard #10

Automatically produce immunization coverage reports by providers, age groups, and geographic areas

Definition The registry has an automated function to assess immunization coverage (e.g., % of children "age-appropriately" immunized) as of a given date for an individual provider's practice, for the registry's entire catchment area, and for subgroups within a practice or the catchment area (e.g., children of a certain age).

To meet this standard: The registry must demonstrate that it can automatically assess immunization coverage as of a given date for an individual provider's practice, for the registry's entire catchment area, and for subgroups within a practice or the catchment area.

Method for certifying function: Review immunization coverage reports by provider, by age group, and by geographic area. Reviewers should ask the registry to demonstrate the function during the site visit.

Data required for review:

- Copy of each type of coverage report generated by the registry

Standard #11

Produce official immunization records

Definition The registry has a function that allows authorized users to produce an individual's immunization history that is accepted as an official immunization record.

To meet this standard: The registry must demonstrate that it can produce an individual's immunization history that is accepted as an official immunization record

Method for certifying function: Reviewers should observe the registry or a provider printing an individual's immunization history that serves as an official record.

Data required for review:

- Copy of the printed official record

Standard #12

Promote accuracy and completeness of registry data.

Definition The registry has developed and implemented a data quality protocol to combine all available information relating to a particular individual into a single, accurate immunization record.

To meet this standard:

1. Registry data accuracy will be measured using a two-step process. The first step will assess the sensitivity (percentage of test case duplicates identified as duplicates by the registry) and specificity (percentage of test cases non-duplicates identified as non-duplicates by the registry) of the registry's automated (pre-human intervention) de-duplication process using CDC's de-duplication test cases.

   During the certification site visit, test cases will be downloaded from CDC's web site and processed by the registry. If the registry 's automated process meets 90% sensitivity and 100% specificity, the second step will occur. Records of the cohort of children born during the 12-month period ending 8 months prior to the site visit will be assessed for duplicates using the registry's automated de-duplication algorithm. A duplicate rate of no more than 5% is required for certification.

2. Where possible, registry data completeness will be measured using the National Immunization Survey (NIS). The NIS provides ongoing national estimates of vaccination coverage among children 19-35 months of age living in the 50 states and 28 selected urban areas[10]. To collect vaccination data for children aged 19--35 months, NIS uses a random-digit--dialing sample of telephone numbers for each survey area. During the survey, parents are asked to allow access to immunization information from all of their child's immunization providers. These providers are then contacted and asked to check their records and provide this information to the survey team. Consent is also solicited to access the appropriate immunization registry for this information. Two measures of completeness will be calculated:

   1) *Population completeness:* the percentage of consented children in the NIS sample with records with at least 2 immunizations in the registry, and
   2) *Immunization history completeness:* for all consented children in the NIS who are also in the registry (with at least 2 immunizations recorded in the registry), the percentage of these children with registry immunization histories that include all vaccines identified in the NIS (i.e., same vaccine type and date recorded for all NIS vaccines identified).

   NIS data quality comparisons will be conducted on an ongoing basis for registries throughout the U.S. Thus information on the registry's population completeness and immunization history completeness should be submitted with the certification application. 80% population completeness and 90% immunization history completeness will be required for certification. In areas where the NIS is not conducted (e.g., U.S. Territories), the alternate methodology below may be used to assess completeness.

3. Alternate methodology. Data collectors will ask the registry to pull a sample of 30 immunization records from each provider site that you will visit. During the provider site visit, data collectors will compare the registry data with that in the provider's records to see if the records match.

[10] *Jefferson County, Alabama; Maricopa County, Arizona; Los Angeles, San Diego County, and Santa Clara, California; District of Columbia (DC); Dade and Duval counties, Florida; Fulton/DeKalb County, Georgia; Chicago, Illinois; Marion County, Indiana; Orleans Parish, Louisiana; Baltimore, Maryland; Boston, Massachusetts; Detroit, Michigan; Newark, New Jersey; New York, New York; Cuyahoga and Franklin counties, Ohio; Philadelphia County, Pennsylvania; Davidson and Shelby counties, Tennessee; Bexar, Dallas, and El Paso counties, and Houston, Texas; King County, Washington; and Milwaukee County, Wisconsin.