

## Hawaii Immunization Registry (HIR) Data Exchange Onboarding Check list

### Phase I: Development

- Received HIR [Flat File](#), [HL7 2.4](#) or [2.5.1](#) Implementation Guide, [HL7 2.4/2.5.1 Reference Tables](#) document, HIR Security Provisions – Data Transfer Tests Only form (see page 5), and [HIR Web Services Data Exchange Setup](#) and [WSDL](#) (if applicable)
- Returned signed HIR Security Provisions – Data Transfer Tests Only form (see page 5)
- Completed Onboarding Form (see page 3) and returned to HIR
- Forms may be faxed to 808-586-8312 or e-mailed to [registryhelp@doh.hawaii.gov](mailto:registryhelp@doh.hawaii.gov)
- Received test account username, password and org code
- Scheduled meeting with HIR staff to discuss development and implementation plans
  1. Required and recommended fields inclusion
  2. Additional required fields for providers receiving state-supplied vaccines
  3. Message Validation Checks (CDC's PHIN Message Quality Framework and HIR <https://phinmqf.cdc.gov/> )
  4. HIR Data Quality (DQ) Checks of messages generated from the EHR in HIR Testing and Production environments
  5. Data exchange set-up
    - Identify pilot sites
    - Timeframe for onboarding
    - Flat File, HL7 2.3.1 / 2.4 or 2.5.1?
    - Manual upload or web service? Note: Web services transmission will only support HL7 file format.
    - The frequency of data uploads and estimated data volume
    - Uni-directional (i.e. Provider to HIR) or bi-directional (i.e. Provider to HIR and HIR to Provider)
    - Will historical immunizations be sent?
    - Expand on relationship and reporting requirements.
  6. Error message return management reviewed & approved
    - How will the EHR manage error messages?
    - How will error messages be displayed to the user?
    - Who will be responsible for reviewing error messages?
    - How will providers correct errors? Using the HIR user interface or correcting error in provider's application and resubmit messages?
  7. Query plans
    - HIR will return only one record per query. If there are multiple possible matches in HIR, no records will be returned.
    - How will returned records be displayed to the user?
    - Will returned records be stored permanently?
    - If storing, will returned records be integrated into EHR immunization history?
    - Will the EHR automatically query for records or will the user initiate the query?
  8. Vaccination Decision Support Inclusion
    - Will HIR vaccination decision support be utilized?
    - How will vaccination decision support information be displayed?
    - Will recommendations be stored?
  9. HIR Notification and Opt-out Requirements
  10. HIR Enrollment and Training Requirements

11. Technical contact, programmatic contact and help desk contact. (where applicable)

## **Phase II: Testing**

- Generated HL7 message from EHR and tested in CDC's PHIN Message Quality Framework (<https://phinmqf.cdc.gov/>) to ensure message is properly formatted to HL7 standards. If submitting Flat File, skip this step.
- Submitted HL7 single patient test message (one patient with one immunization) to HIR Testing environment.
- Completed HIR DQ Check in HIR Testing environment
  - Received list of HIR DQ test patients and enter information into EHR
  - Submitted Flat File or HL7 test message with unique patient data (i.e. different patient name, date of birth and address) to HIR Testing environment
  - Printed screenshots of demographic and immunization screens in EHR for each test patient
  - Uploaded the test message to HIR Testing environment and e-mailed/faxed screenshots to HIR staff for DQ validation
- Completed web services set-up and validation (if applicable)
  - Sent certificate request (CSR) to [registryhelp@doh.hawaii.gov](mailto:registryhelp@doh.hawaii.gov)
  - Received a signed certificate and installed it
  - Completed web service set-up
  - Submitted additional test messages to validate connectivity

## **Phase III: Training**

- Provided HIR the complete list of facilities.
- Submitted HIR Annual Facility Enrollment Application Form for each facility
- Submitted HIR Confidentiality and Security Statement for each HIR user
- Completed notification/opt-out conference call with HIR Trainer

## **Phase IV: Go-Live and Rollout**

- Discussed plans for rollout with HIR staff
- Received HIR provider org IDs for all facilities
- Completed HIR Production environment DQ check
  - Identified ~20 patients from first day/week of go-live to be DQ checked
  - Printed screenshots of demographic and immunization screens in EHR for each patient and faxed screenshots to HIR staff for DQ validation
- Rollout

## **Phase V: Maintenance**

- Notify HIR Help Desk of system or personnel changes
- Periodic DQ reviews
- Annual enrollment renewal

# HIR Data Exchange On-Boarding Form

Form may be faxed to 808-586-8312 or e-mailed to [registryhelp@doh.hawaii.gov](mailto:registryhelp@doh.hawaii.gov)

1. Org ID#/Site Name: \_\_\_\_\_
  
2. Is this site a vendor/parent org?                       Yes                       No
  - a. If yes, list org ID#s or attach spreadsheet of child clinic name/address: \_\_\_\_\_  
\_\_\_\_\_

## Contact Info:

3. Primary Contact:  
Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
Phone #: \_\_\_\_\_  
Email: \_\_\_\_\_
  
4. Clinical Contact:  
Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
Phone#: \_\_\_\_\_  
Email: \_\_\_\_\_
  
5. Technical Contact:  
Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
Phone #: \_\_\_\_\_  
Email: \_\_\_\_\_
  
6. Data Exchange / HL7 Modification Contact:  
Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
Phone #: \_\_\_\_\_  
Email: \_\_\_\_\_
  
7. Data Exchange Error Review Contact:  
Name: \_\_\_\_\_  
Title: \_\_\_\_\_  
Phone #: \_\_\_\_\_  
Email: \_\_\_\_\_
  
8. Vendor/Consultant:  
Contact Name: \_\_\_\_\_  
Contact Title: \_\_\_\_\_  
Contact Phone #: \_\_\_\_\_  
Contact Email: \_\_\_\_\_

9. Do you have internal IT staff?  Yes  No
10. Do you use external expertise?  Yes  No
11. Participation in Meaningful Use:
- a. Stage 1:  Yes  No
- b. Stage 2:  Yes  No
- c. Stage 3:  Yes  No
12. Participation in the VFC Program:
- a. VFC PIN: \_\_\_\_\_
- b. Ability to capture dose-level eligibility:  Yes  No
13. Utilizes a test environment with test patients:  Yes  No
14. Familiar with using SOAP web services:  Yes  No
15. Electronic Health Record Vendor
- a. EHR Product: \_\_\_\_\_
- b. EHR Version: \_\_\_\_\_
16. File Format/Method of data exchange:
- | <u>File Format</u>                       | <u>Method</u>                                     |
|--|---|
| <input type="checkbox"/> Flat File       | <input type="checkbox"/> Manual upload            |
| <input type="checkbox"/> HL7 2.3.1 / 2.4 | <input type="checkbox"/> Real Time – Web Services |
| <input type="checkbox"/> HL7 2.5.1       |   |
17. EHR collects historical shot information:  Yes  No
18. EHR capable of creating HL7 messages:  Yes  No
19. EHR capable of bi-directional data exchange:  Yes  No
20. EHR is hosted:  Internally  Externally
21. EHR supports real-time messaging:  Yes  No

# Hawaii Immunization Registry (HIR) Data Transfer Security Form

Fax form to 808-586-8312 or e-mail to [registryhelp@doh.hawaii.gov](mailto:registryhelp@doh.hawaii.gov)

Organization Name: \_\_\_\_\_

User Name: \_\_\_\_\_  
Last Name First Name Middle Initial(s)

Physical Address: \_\_\_\_\_  
Number and Street Name (No P.O. Boxes)

City State Zip Code

Mailing Address: \_\_\_\_\_  
Number and Street Name (No P.O. Boxes)

City State Zip Code

Email Address: \_\_\_\_\_

Telephone: ( ) \_\_\_\_\_ Ext.: \_\_\_\_\_ Fax: ( ) \_\_\_\_\_

If you are an EHR/EMR/Vendor/HHIE submitting on behalf of a provider, complete Section I, otherwise proceed to Section II.

## Section I:

Please describe your Organization's relationship with provider's data:

- Electronic health record vendor developing interface
- Contractor developing interface
- Other: \_\_\_\_\_

Name of person responsible for the SSL/TLS/SOAP Username and Password: \_\_\_\_\_

Please complete the following questions:

- |  |                              |                             |
|--|------------------------------|-----------------------------|
| 1) The provider's data is physically stored within my organization                 | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| 2) My organization is responsible for the transfer of provider's data to HIR       | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| 3) The provider's data transfers to HIR through my organization                    | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| 4) My organization is able to see the provider's data at any point during transfer | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| 5) My organization is planning to or is able to keep a copy of provider's data     | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| 6) My organization may log into HIR  | <input type="checkbox"/> Yes | <input type="checkbox"/> No |

If all of the questions above are "No", sign and return form to the above fax or email, otherwise proceed to Section II.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

## Section II:

As a condition of authorized access to the Hawaii Immunization Registry (hereinafter referred to as “the Registry” or “Registry”) for the purpose of data transfer, I AGREE TO COMPLY WITH THE FOLLOWING REQUIREMENTS:

### I. Information Access Management

- A. Each authorized user shall be assigned an account to access the Registry and shall be prohibited from sharing this account.
- B. Users shall be held accountable for actions performed with their assigned account.
- C. 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.
- D. Accounts that have been inactive for 90 days shall be disabled.

### II. Security Awareness

#### A. Password Management

All passwords for accounts shall be constructed in accordance with the following Registry password management specifications. Periodic verification of compliance with these specifications shall be conducted.

- 1. All accounts shall have a password expiration date.
- 2. All stored passwords shall be encrypted.
- 3. Passwords shall NOT be shared.
- 4. Password cracking is strictly forbidden.
- 5. Rules for password configuration:
  - a. Include a minimum of eight (8) characters
  - b. Use numbers and both upper and lower case letters
  - c. Do not include names, dictionary words (English or foreign), or the user's ID or birthday
  - d. Do not include common sequences that can be found on a computer keyboard

### III. Workstation Use

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

  - 1. Workstations shall be located in a secure area.
  - 2. Workstations shall be outfitted with appropriate electrical power conditioning, surge protection, and backup power appliances.
  - 3. Screensavers shall be set to lock automatically after ten (10) minutes of system inactivity.
  - 4. Screensavers shall be password protected.
  - 5. Workstation screens shall be locked whenever a user steps away from them.
  - 6. 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.
  - 7. Ability to boot from floppy drive or CD ROM shall be disabled.
  - 8. The same policies for workstations apply to laptops and other mobile devices; additional

considerations include:

- a. Extra protection such as a lockable cable, usually designed specifically for laptops, shall be used to secure the laptop at all times when unattended.

#### IV. Access Control

- A. Authorized users shall be assigned a unique user name.
  1. Users shall not directly or by implication employ a false identity (i.e. use the name or electronic identification of another).
  2. 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.
  3. Users are responsible for ensuring that their User ID and password are not disclosed to third parties.

#### V. Integrity

- A. **Person or Entity Authentication**
  1. 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.
  2. Authorized users shall not have access to the Registry from more than two workstations simultaneously.

#### VI. Transmission Security

- A. The Department of Health shall ensure that the Registry System is configured to prevent unauthorized access and modification of information as it is transmitted over an electronic communications network (e.g. Internet) via the following:
  1. Registry information shall be encrypted when electronically transmitted, copied, or transferred.
  2. All traffic between the web server and client browsers shall be encrypted (minimum 128-bit encryption level).
  3. The Registry System shall encrypt data prior to sending through a secure (HTTPS) data transport.
  4. The Registry System shall be configured to ensure secure real time data exchanges.
  5. 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.
  6. Any connection to the Registry System shall occur through controlled interfaces.
  7. Network connections shall be properly terminated at the end of user sessions.
  8. Network connections shall be terminated automatically upon a specified period of inactivity or other identified events.
  9. Intrusion tools and techniques shall be utilized to provide real-time identification of any unauthorized use, misuse, and abuse of the Registry System.

I shall not add, delete, alter, manipulate or disclose data that I am responsible for transferring to or that is stored in the Hawaii Immunization Registry.

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
Signature - User Date

\_\_\_\_\_  
Title