Consumer Access to Immunization Information System (IIS) Data: A Guide for Consumer Access via an IIS Portal

December 16, 2013

Contents

1 Introduction

1.1 Project Background

For over twenty years, state and local jurisdictions have been collecting immunizations in a centralized database originally referred to as an Immunization Registries but more commonly referred to as Immunization Information Systems (IIS). The Centers for Disease control and Prevention (CDC) defines IIS as, "confidential, population-based, computerized databases that record all immunization doses administered by participating providers to persons residing within a given geopolitical area."[1]

Individual/consumer access to immunization registry data has recently been identified as a priority initiative of the Office of the National Coordinator for Health Information Technology (ONC), the CDC, and many state immunization program. However, there are a number of challenges to overcome to allow individual access to IIS data. These include policy, technology, identity proofing, communication and outreach. The response by some states has been to grant access by creating a duplicate database for access. Some others states are investigating portals or EHR/PHR solutions. While it is clear that there are as many options as there are challenges to consumer access, the goal of providing access to consumers to enhance their health care engagement is a priority. The ONC strongly encourages the development of tools and applications to make this actionable.

Nearly twenty states use IIS applications based on the Wisconsin Immunization Registry (WIR) software. WIR is a web based system that provides documentation and access to information about immunization records for patients. Updates to the system can be done by providers through numerous methods - manual entry through the web based client, through HL7 standard messaging or through a flat or delimited file batch process. WIR collects data about immunizations and offers providers an immunization history and forecast for each patient. The forecast lays out a treatment plan to assist providers in administering immunizations.

A group of WIR states worked together to identify common approaches and best practices that could be used to provide individual access to IIS data in support of Federal consumer health data initiatives. This work built upon an earlier study conducted by the State of Minnesota, one of the participating states in this effort. After compiling a report detailing the information known to date, the project team conducted a series of internal webinars and surveys, as well as external interviews, to identify business requirements and options for IIS access. A set of guiding principles was also developed to help the team narrow the set of possible options for IIS direct access, and access through EHRs/PHRs.

The laws, policies, and technical standards of the participating jurisdictions differ, so no "one size fits all" solution to IIS access was defined. The project described a wide variety of potential solutions – some feasible today, some less so – as a way to spur discussion and consider all

---

[1] http://www.cdc.gov/vaccines/programs/iis/about.html

possibilities. The proposed IIS direct-control solution leverages HL7 web services for IIS query/response that are aggressively being deployed around the country and was not specific to WIR-based projects; solutions using this technology are already becoming available in the market.[2] The proposed EHR/PHR indirect-control solution leverages patient view/download/transmit requirements of Stage 2 Meaningful Use as a way to encourage providers to offer access to these data.

1.2 Federal Context

The CMS EHR Incentive Programs provide another backdrop for consumer access to immunization data.[3] Established in 2010, the incentive programs encourage eligible professionals and hospitals to implement health information technology. The primary focus of this program is the implementation of electronic health record systems and their "meaningful use" (MU). This multi-year program will roll out in several phases, or "stages." A critical component of the programs is a set of public health objectives related to reporting, with corresponding measures and standards, which eligible professionals and hospitals will be expected to support if the public health agencies in their jurisdictions are capable of exchanging data electronically. Immunization reporting was established as an optional, or "menu set" item, in Stage 1 of the program, before being elevated to a required, "core set" item in Stage 2 which begins in 2014.

The Stage 2 Eligible Professional (EP) MU Core Measure 7 outlines the Patient Electronic Access. The objective states that the provider must "Provide patients the ability to view online, download and transmit their health information within four business days of the information being available to the EP."[4] It further defines the meaning of access, view and transmission as stated below.

"View/Download/Transmit" represents a new, more formal requirement for patients to access their own health data ostensibly through the provider's EHR system. Blue Button/Blue Button+ may become one strategy for providing this access. As IIS contemplate strategies for providing data access directly to consumers, these initiatives may provide strong points of leverage in accomplishing this goal.

National IIS policy originates with the National Center for Immunization and Respiratory Diseases (NCIRD), a branch of the CDC. As stated above, the CDC echoed the sentiments of several states HLN interviewed that the demand for direct access to immunization records does not appear to be coming directly from the consumer at this time. The demand for this service is coming from the top: the Secretary of Health and Human Services and the National Coordinator for Health Information Technology at ONC as a function of their consumer empowerment

---

[2] For a good example, see https://myir.net/

[3] http://healthit.hhs.gov/portal/server.pt?open=512&objID=2996&mode=2

[4] http://www.gp; o.gov/fdsys/pkg/FR-2012-09-04/pdf/2012-21050.pdf#12

initiative. This initiative is part of a large Federal initiative related to consumer access to data that transcends health care.[5]

1.3 Purpose of this document

Since the EHR and PHR markets are still maturing, the capabilities for consumer access through these mechanisms are not solidified. The purpose of this document is to provide a guide for IIS portal development.   A viable IIS portal solution leverages HL7 web services for IIS query/response that are aggressively being deployed around the country and is not specific to WIR-based projects. The guide provides details of two alternate options that were vetted by the participating WIR states. The guide addresses issues of promising practices and guidelines for implementation.

2 Requirements for Consumer Access

Based on the research and discussion conducted by the Project the following core requirements were identified:

1. **Support for Federal consumer health data access initiative** as referred to above. This is an evolving set of initiatives and may or may not imply specific strategies.
2. **Query access is provided for a patient's record.** While this may sound obvious, it is at the core of what this project is intended to address.
3. **Query returns one and only one target record.** When providers access an IIS, they can typically enter search criteria that may yield multiple, potential patients' records. For consumers, however, they must know enough about a unique record to establish a single match in response to a query.
4. **Query response does not return demographic data that was not originally supplied in the query parameters.** The project is very sensitive to the need to provide immunization data but little else back to a consumer that might prove to be a violation of patient privacy.
5. **Only authorized users can see data for a particular patient.** User relationship to patient is either established reliably before the query or user knows enough data about the patient to substantiate the relationship with the patient.
6. **If the solution requires authentication then single-factor authentication is sufficient for this project.** ONC indicates that two-factor authentication is recommended, and perhaps required, for access to patient records, but this may not be practical in this scenario.
7. **User can view consolidated, de-duplicated immunization history** (at a minimum, series, vaccine, and date), indicator of validity for each dose, and, potentially, **a forecast of doses due** (and overdue if algorithm provides this distinction). This view of the data may be simpler than what a provider sees currently through their IIS, or through their local EHR system, but is sufficient for a patient.

---

[5] http://www.data.gov/

8. **User can generate or download a report with vaccine history suitable for school, camp, or child care admission.** This is a key requirement, and is often the reason why parents and adult students want access to these data in the first place.

These items were viewed by the project as *minimum,* or core requirements; additional requirements may be imposed by particular jurisdictions.

3 Principles for Option Selection

The project considered both short and long term solutions and determined that both the IIS portal solution and EHR/PHR solution could be investigated as a strategy, depending on the resources devoted to implementation by individual states. The following principles were used by the project in selecting options and should be upheld to the degree possible within any solution that is deployed:

- **Meet Requirements**: Recommended options should meet all the core requirements and as many of the other requirements as possible (see section 2 above).
- **High leverage:** Recommended options should leverage existing (and planned) IIS and non-IIS activities wherever possible.
- **Consistency with National Standards:** Recommended options should be consistent with national standards and directions both within and outside of the IIS community. It is recognized that some elements of the national scene may not yet be certain.
- **Recognize Diversity:** We need to recognize the diversity in both IIS implementation and state and local laws/regulations. There is no "one size fits all" solution, so multiple recommended strategies are expected. On the other hand, too many options will degrade our focus and distract progress.
- **Feasibility:** Recommended options should be investigated if the state has the resources to feasibly implement the solution within one year of project commencement.
- **Cost:** Recommended options should be cost-effective, especially since it may be an interim solution. Cost should include total cost of ownership, including ongoing maintenance, and transition to longer-term solutions.
- **Incremental Steps:** We should recognize that it will likely take incremental steps to move us in the direction we want to go. But, there may be a tension between short-term and long-term strategies.

4 Solution Description

4.1 Introduction

The WIR State workgroup developed two alternate options worthy of further exploration and/or pilot testing for web based access directly against the IIS. The direct-access option preferred by the group involves developing a portal to allow consumers to directly query the IIS system. Within this strategy the workgroup has defined two alternative workflows that provide

options for the search criteria and how the query response will be returned. There are many reasons why this solution is valuable:

- Allows individual states to determine the search criteria for the query. Queries can be made based on "what you know" or based with a PIN number assigned by the provider or by the IIS.
- Takes advantage of an HL7 query against the IIS which is readily accessible by IIS systems.
- Allows for a real-time or delayed query response based on the state's capability of running real-time or batch QBPs.
- Allows the states to determine if the query response is sent to the person making the query or directed to a "person of record" already identified in the IIS.
- Promotes best practice by requiring unique searches for each person in the IIS.
- Allows States to filter adolescent data, including sexual health data, if required by state or local law.
- Allows States to provide a selection of report options that may or may not include personally-identifiable health information such as address, phone or location of immunization.
- Allows for incorporation of Blue Button and/or Blue Button+ capabilities (though these options were deemed out of scope by the work group).

Indiana's CHIRP, Children and Hoosier Immunization Program, concluded that consumer access to data should be through a secondary portal. In July 2012 they announced the MyVAX Indiana web portal to allow individuals direct access to their immunization records. Individuals receive a PIN number from their provider. This method of authentication was selected because of the strong patient-provider relationship. Individuals can print an official record with history and forecast. No PHI or provider location is included. MyVAX Indiana has incorporated the Blue Button logo to enable people to download as text, PDF or HL7.[6,7]

4.2 Work Flow for Person of Record - Option 1

The first called *Person of Record* option allows the consumer to query the system for themselves or someone else based on information that they know. This option then uses the *Person of Record* already on file in the IIS to ensure that the query response is send to the known person of record (in the case of minors, often the parent or guardian). All query responses are emailed to the Person of Record only.

The basic work flow for direct access to the IIS is displayed in the figures below. There are several preconditions for this work flow:

---

[6] https://myvaxindiana.in.gov/
[7] http://www.health.state.mn.us/e-health/patientengage.html

- The patient (or legal guardian) can provide enough information about themselves or their dependent to perform a search that will return one and only one match from the IIS.
- The Person of Record information has been given to the patient's provider for uploading to the IIS from the EHR if the State is using Person of Record email option.
- The IIS is abiding to any consent requirements before sharing adolescent health data.
- The IIS portal receives one query per patient data request. Batch queries are not supported.
- The IIS portal follows appropriate privacy and security best practices once identifiable health data is presented to the patient.
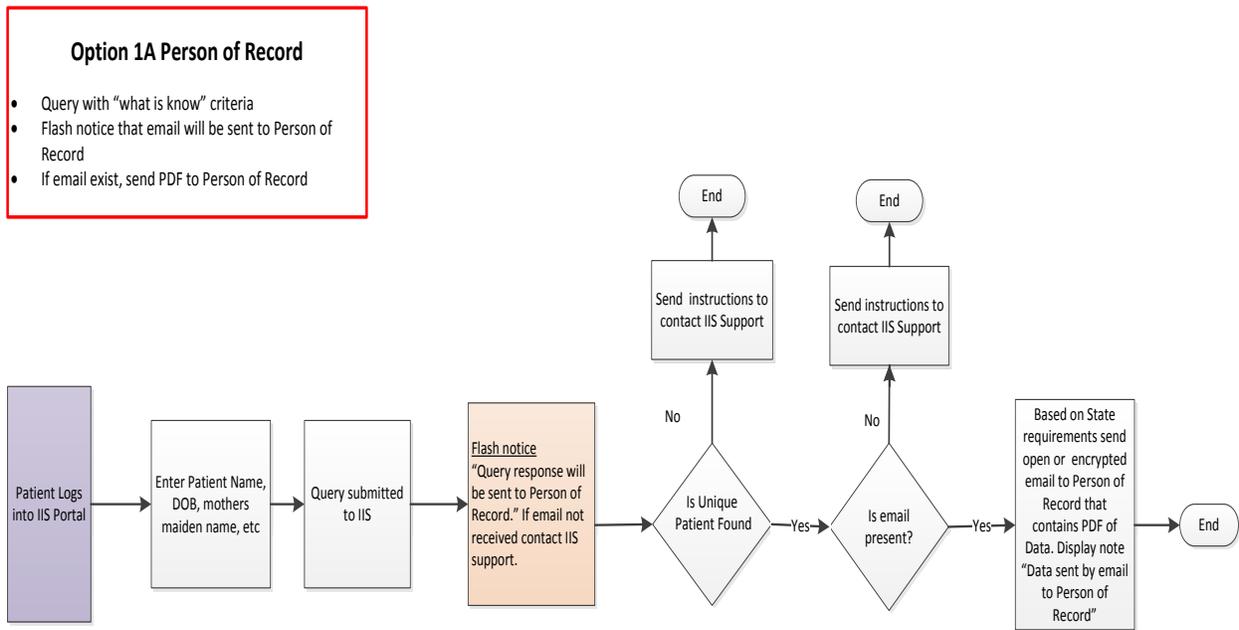

Figure 1 – Workflow of Person of Record

- Consumer logs into the IIS portal from any browser.
- Consumer provides name and/or email address.
- Portal captures the requestor information along with the IP address and the timestamp for an IIS audit file.
- Consumer creates query search by adding information about themselves or any other individual based on "what they know." The search criteria will be determined based on State requirements to produce a unique match. Criteria might include: Name, DOB, Address, and Mother's maiden name, etc.
- The HL7 QBP query is run against the IIS.
- Screen message will flash stating "Query response will be sent to Person of Record. If you have any questions or the email does not arrive in x hours please contact your IIS Support staff" (or a similar message as authored by the IIS project).

- If query does not return a unique patient, the query is terminated and the consumer is requested to contact the IIS Support team or retry.
- If unique patient is found, IIS checks for Person of Record. If email address is not found, instructions are sent to the consumer to contact their IIS Support team for information on how to add Person of Record to account.
- If State requires filtering of adolescent health data, this information is redacted from the PDF.
- If an email address of Person of Record is found, an encrypted or non-encrypted email (based on State requirements) is sent the email address of the Person of Record.

4.3 Work Flow for Requestor Response - Option 2

The second option called *Requestor Response* allows for two search criteria options to locate the patient. The first search is based on "what you know" and the second search option is based on a PIN number assigned by the provider or IIS support. The *Requestor Response* renders the official immunization history/forecast/report for the requestor and allows them to select print, download and or fax option.

The basic work flow for direct access to the IIS is displayed in the figures below. There are several preconditions for this work flow:

- The patient (or legal guardian) has already received credentials to perform a search if the State is using a PIN as part of its search criteria.
- The patient (or legal guardian) can provide enough information about themselves or their dependent to perform a search that will return one and only one match from the IIS.
- The IIS is abiding to any consent requirements before sharing adolescent health data.
- The IIS portal receives one query per patient data request. Batch queries are not supported.
- The IIS portal follows appropriate privacy and security best practices once identifiable health data is presented to the patient.

Workflow of Requestor Response

Option 1B Requestor Response

- Search either by "what is known" criteria or by PIN issued by provider or IIS Support.
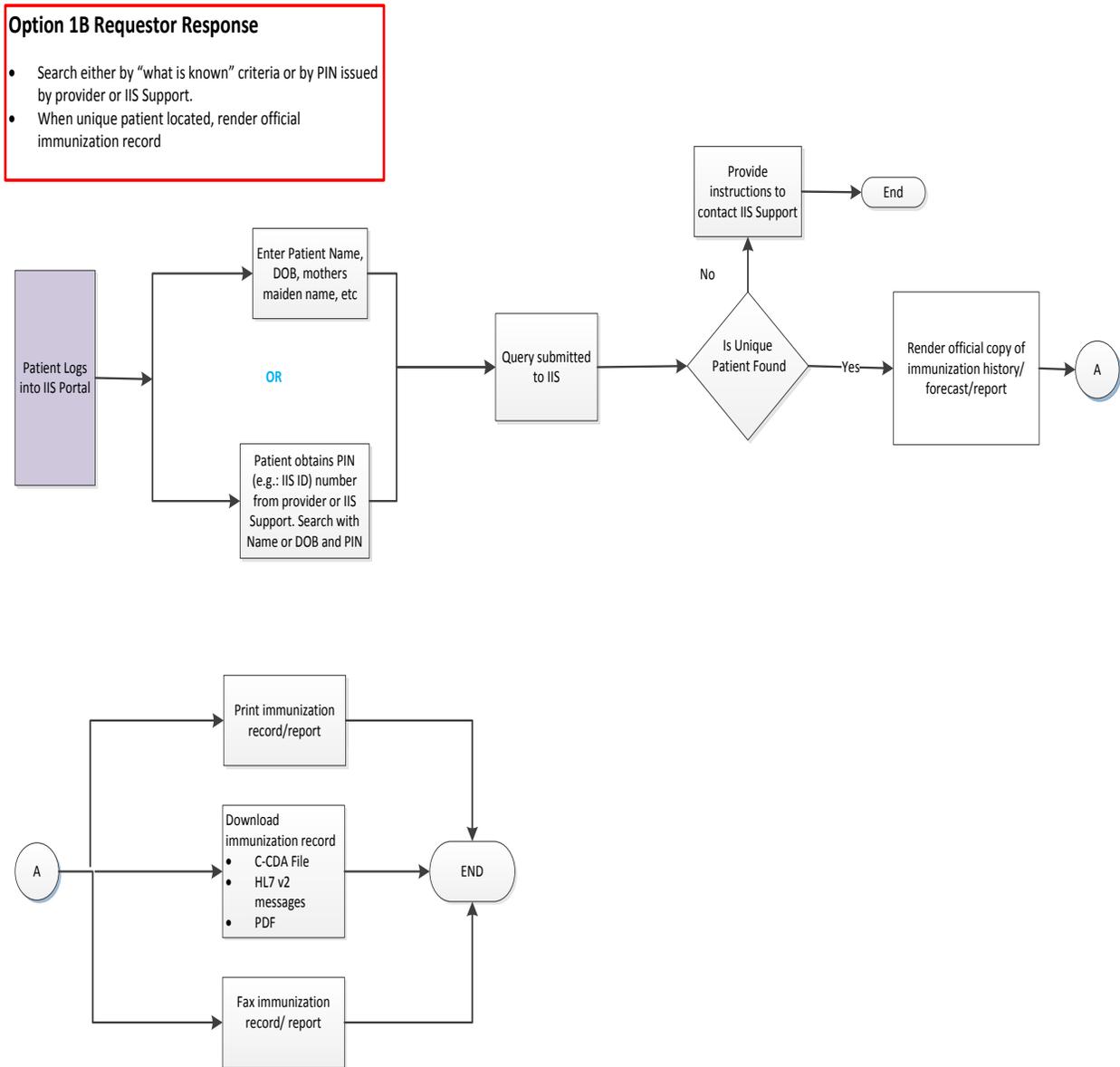- When unique patient located, render official immunization record

Figure 2 – Workflow of Requester Response

- Consumer logs into the IIS portal from any browser.
- Consumer provides name and/or email address.
- Portal captures the requestor information along with the IP address and the timestamp for an IIS audit file.
- Consumer creates query search by providing "what they know" or by entering a PIN and patient's name/Date of Birth.
- The HL7 QBP query is run against the IIS.

- If query does not return a unique patient, the query is terminated and the consumer is requested to contact the IIS Support team or retry.
- If State requires filtering of adolescent health data, this information is redacted from report.
- Render official copy of immunization history/forecast/report.

4.4 Multi-State Portal Use

This document outlines an IIS portal that can be implemented by an individual state. Similar to the portal used by Indiana, each state could develop and deploy a portal to their IIS. Individual portal development allows for customization of look and feel, the search criteria, the audit logs and support screens as well as for the defined reports available to the consumers.

The WIR work group discussed the possibility for joint development of a multiple state portal that could be used by consumers from many (or potentially even all) states accessing an IIS. The advantage of this shared portal would be to share the burden and cost of the development. However the disadvantages to this approach are the State and local requirements imposed by each Registry and the need to manage and fund a larger, more complex project. The details of a joint development project were not thoroughly discussed.

4.5 Issues to Consider

There are a number of important issues and choices IIS partners need to make in order for a solution to be effective in a given settings:

	Issue/Key Question	Suggested Guidance
Technical	States need to have audit logs of requestors. This information might include requestors' name/email, IP address and timestamp. Information would include data provided by the consumer as well as the consumer IP address and a timestamp.	This is an administrative feature of a portal. For single use portal, this information can be collected with the portal for audit logs. For a multiple state portal, access to this audit log information would have to be provided via administrative features of the application.
Privacy and Security	Consumer access queries against the IIS must return one unique record. In states where the SSN and/or Medicaid number is not supported for data searches consumers must have enough information to success submit a query and get one and only one response.	Each state will need to provide criteria to consumers to allow for a unique search. Where SSN or Medicaid ID are not available in the IIS, states should consider making the internal IIS ID known to the provider and the patient to facilitate searches.
	Potential exposure of personally-identifiable health information in electronic form in patients hands may be increased as immunization data may be combined with more sensitive health	Educate patients about information privacy and security and the risks that come from even possessing unencrypted copies of electronic health information.

Issue/Key Question	Suggested Guidance
information.	
Jurisdictional law may prevent patient access to IIS data.	Work with public health agencies to change legislation to allow this access.
Delivery of an immunization record in unencrypted e-mail may violate privacy and security standards or best practice and potentially lead to an inappropriate disclosure of identified health information.	Each state should provide a secure e-mail service (*e.g.,* Direct) that will encrypt the message. Consumers would receive a plain-text e-mail that they have received a secure message from the portal and would be directed as to how to read this message in a secure manner.
Consumer may sometimes want an "official record" for school and sometimes want the forecast for planning.	A State could provide a list of reports that can be returned as a result of the query. This list should be available at the time of query. In some states there may only be one option.
If the Person for Record is not available in the IIS, then the query response cannot be sent.	VXU messages sent by EHR vendor systems for data submission to the IIS will be required to populate the Person of Record information for states using this option.
If Person of Record is not populated or is incorrect, the consumer is directed to IIS support.	The IIS help desk must have established protocols for adding or changing the Person of Record, including an authentication or authorization process.

The left column cells for the last three rows are labeled "Functional" (rotated).