Consumer Access to Immunization Information System (IIS) Data

Synthesis of Work to Date

August 2013

Table of Contents

1 Executive Summary

For over twenty years, states and other jurisdictions have been collecting data about immunizations for an entire population in a common, shared database originally referred to as an Immunization Registry but more commonly referred to as an Immunization Information System (IIS). 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 Centers for Disease Control and Prevention (CDC), and the state immunization program. However, there are a number of legal and technical challenges to overcome to allow individual access to IIS data.

States are seeking options and strategies for direct consumer access to immunization information in response to a top down initiative that has been launched by the White House to provide consumers with direct access to their health records. Deloitte's partner on this engagement, HLN Consulting, LLC (referred to as HLN in the remainder of the document), has performed a series of interviews and conducted research to determine what a handful of states are doing to fulfill this need for their constituencies. The research and interviews were designed to paint a broad brush on the legal, technical and policy issues surrounding access to a state IIS. The goal of the research, readings and interviews was to determine how various federal and state organizations and vendors are addressing this issue of direct consumer access to immunization information and how they are overcoming the challenges of access authentication and proxy.

HLN developed the following sets of requirements for providing consumer access to immunization data. In addition, HLN identified some particular limitations which may also affect viable solutions to this project which should be considered when considering strategies. HLN examined all available material and developed the following set of options for IIS consumer access relevant to the Wisconsin Immunization Registry (WIR) software that is in use in several states. The conclusions and recommendations include:

- Unless outreach into the community has been done to determine if this functionality is desired or demanded, significant investment in a consumer access strategy should be limited until a purposeful engagement with consumers or consumer advocate organizations takes place.
- States that have provided consumer access have done so with little up-front cost and little to no impact on current IIS operations or system performance.
- The EHR market is not yet very sophisticated in terms of patient access, but the impending implementation of MU Stage 2's "view/download/transmit" measure may quickly change this. Dominance of a particular EHR system vendor in a given market could provide some leverage in that particular space. State and local public health agencies (PHA) may provide a point of access for patients without a medical home.
- State and public health agency technical, legal, and information security staff members should be fairly involved in IIS operations and decision-making so any move toward providing consumer access will require the scrutiny of these offices. This may limit IIS' ability to move forward quickly or easily.

- If there is no unique identifiers in the IIS known easily to the outside community (Social Security Number (SSN), Medicaid ID, Medical Record Number (MRN)), consumer access cannot be provided without some level of effort, technical or administrative. Note: Indiana's PIN access was not achieved using WIR software.
- User identity proofing issues for consumer access are somewhat of a red herring: The tough part is not independent user authentication but rather user *authorization*, *i.e.,* establishing the user's relationship to the patient. This is difficult to do in an IIS alone without corroborating that relationship with data in the IIS or validating that independently with another source (like the provider).
- In terms of the implementation options identified in the report, it may be challenging for a PHA to expand the use of the WIR software web client for consumer access. Creation of a mobile app is probably the most forward-thinking in terms of consumer access and emerging technology usage patterns, though the difficulty in printing a formatted report from a mobile device may be a real barrier. Permitted access via query from electronic health record (EHR) and/or personal health record (PHR) systems require the least modification to operations and software, but require close cooperation with the vendors and sites. Pursuit of a Blue Button+ strategy allowing patients to "subscribe" to records in IIS is the most forward-thinking of all the options.

2 Introduction and Background

2.1 Scoping the Issue

For over twenty years, states and other jurisdictions have been collecting data about immunizations for an entire population in a common, shared database originally referred to as an Immunization Registry but more commonly referred to as an Immunization Information System (IIS). The CDC defines an IIS as a, "confidential, population-based, computerized databases that record all immunization doses administered by participating providers to persons residing within a given geopolitical area."[1] Nearly twenty states use IIS applications based on the WIR software application which is in use (in one form or another).

Individual/consumer access to immunization registry data has recently been identified as a priority initiative of the ONC, the CDC, and the state immunization program. However, there are a number of challenges to overcome to allow individual access to IIS data. Rear Admiral Ann Schuchat, MD spoke at the Markle Foundation's 2012 Consumer Health IT Summit and addressed the challenges of consumer access to health records. She discussed the barriers for consumer access to immunization 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 PHR/EHR 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.

Several WIR states are investigating the opportunity for consumer access to their immunization registration data in support of Federal consumer health data initiatives. 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. These include manual entry through the web based client, through HL7 standard messaging, through a flat file batch process or through a flu vaccine spreadsheet. 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.

2.2 Federal Perspective

The ONC is looking at many different strategies to address consumer access to health care data. While the original release of Health Insurance Portability and Accountability Act (HIPAA) in 1996 guaranteed the right of access to personal health care information, access to this data still presents many technological challenges and consumer demand is marginal. The Centers for Medicare & Medicaid Services (CMS) EHR Incentive Program's Meaningful Use (MU) encourages enhanced patient engagement and consumer access. The ONC has recently posted a web page seeking the public's input on Federal Consumer e-Health Strategies. This page details the ONC's "3 A's" of

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

consumer engagement: **A**ccess, **A**ction and **A**ttitude.[2] It states that when patients have the ability to review and update their health record they become active participants in their health care. A recently conducted Deloitte survey stated that 60% of people interviewed would consider changing their health care provider if they could access their health care records.[3]

One of the solutions to provide consumer access to health records is the Blue Button Initiative. The Blue Button Initiative was launched in 2010 for the Veterans Administration from the MyHealtheVet portal.[4] The application was developed to allow Veterans to easily access and download their medical data for their own use or to share it with other medical providers. The guideline for the data in Blue Button was that it had to be both human and computer readable. Blue Button was branded and the icon represents a mechanism to view and/or download personal health data in a wider variety of settings. Its use continues to grow and this year reports its one-millionth user. The 2011 campaign by the U.S. Department of Veterans Affairs (VA) encouraged widespread use of this technology and encouraged vendors and developers to create applications to enhance the use of this data. Health care providers and organizations are encouraged to use this technology on their web page to promote easy access to data.[5]

In 2013 ONC released Blue Button+ (BB+) which extended the original Blue Button Initiative.[6] This initiative provides for digital access to health information. Specifications and use cases have been developed through the Standards and Interoperability (S&I) Framework process. The BB+ initiative encourages the use of structure data and intentionally allows the market place to determine how and what types of tools should be developed.

The CMS EHR Incentive Programs provide another backdrop for consumer access to immunization data.[7] 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, established as a "menu set," or optional, measure is Stage 1 of the program, was elevated to a "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."[8] 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

[2] http://content.healthaffairs.org/content/32/2/376.abstract
[3] ONC's Strategy for Engaging Consumers - 2012 Consumer Health IT Summit
[4] http://www.va.gov/bluebutton/
[5] http://bluebuttondata.org/
[6] http://bluebuttonplus.org/
[7] http://healthit.hhs.gov/portal/server.pt?open=512&objID=2996&mode=2
[8] http://www.gpo.gov/fdsys/pkg/FR-2012-09-04/pdf/2012-21050.pdf#12

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 initiative. This initiative is part of a large Federal initiative related to consumer access to data that transcends health care.[9]

Based on HLN's interviews, the CDC, NCIRD explains that the push for consumer access is a "top down" initiative as a function of public access interest. From the CDC perspective, the biggest concern for the IIS programs is the lack of tools to ensure identity proofing of consumers (see section six below). This issue may be addressed by EHRs/PHRs in the future as part of meaningful use requirements. However at this time consumer access is not a high priority for IISs across the country and is not an explicit demand of the community. As EHRs roll out more portals and authentication issues are addressed, the desire for consumer access will likely grow and IIS priorities may change.

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

3 Requirements and Limitations

Through discussion, research, and analysis, HLN developed the following sets of requirements for providing consumer access to immunization data. These requirements should be used to assess the "fit" of the strategy options in the next section as solutions for this project. The core requirements listed first should be absolute requirements; the "other possible requirements" maybe considered optional at this time.

Core Requirements

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. **User can query for a patient's record.** While this may sound obvious, it is at the core of what this project is about.
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. **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.
5. **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.
6. **User can view consolidated, de-duplicated immunization history** (at a minimum, series, vaccine, and date), indicator of validity for each dose, **and 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.
7. **User can download immunization history and forecast in a standard, electronic format.** This is consistent with the "view/download/transmit" objective of Stage 2 MU.
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 this data in the first place.

Other Possible Requirements

1. **Allow consumers to indicate potential errors in IIS records for follow-up with providers and possible correction.** Patients have this right under HIPAA with respect to their provider-based patient records, but have no specific right to this functionality with respect to data stored in the IIS. Data quality is an ongoing issue to be managed, and enlisting patients in this process can only improve overall data quality. IIS need to consider, however, the resources that might be necessary to follow up on these additional data quality questions should any surface.
2. **Generate reminder/recall notices to "push" to parents electronically.** A patient report (see core requirement 8 above) should provide a forecast of immunizations due at the moment the report is generated, but because the forecast changes as the patient ages it may

also be beneficial to "push" a notice in real time. This must be done securely, however, to ensure that protected health information (PHI) is not transmitted over an unencrypted network or stored unencrypted at an insecure end-point.

Potential Limitations

In addition to the requirements above, IIS's may have some particular limitations which may also affect viable solutions to this project which should be considered when considering strategies. Below is a list of some of the potential limitations. This is not an exhaustive list as individual state statutes vary and will have varying impact on access capabilities and restrictions.

1. **No explicit demand from the community for this functionality.** In most states there has been no groundswell of consumer demand for this access. On the other hand, there has been no consumer education around this potential functionality so there may be no basis for consumers to request it.
2. **Search criteria may have restrictions.** Some states prohibit the use of SSN or Medicaid ID as part of the patient demographics. Use of these (ostensibly) unique identifiers would facilitate the return of one and only one record in response to a query (see core requirement three above); absence of these identifiers makes this a bit more challenging, especially in the case of common names.
3. **Little to no use of HL7 query to date.** Some of the potential solutions described below leverage the state IIS's current ability to receive and respond to standard HL7 v2 message queries and return patient immunization histories and forecasts. While this may provide a significant point of leverage for one or more solutions, this query capability currently has very limited use in some provider communities.
4. **No *official* Parent Report exists.** Some IIS lack an official report used for school, day care, or camp entrance. An official report would certainly provide more leverage for this project.

4 Current Consumer Access to IIS in the US

To gather an understanding of how states were providing access to IIS data interviews were held with three states providing consumer access through their IIS software. These states included Wisconsin, Nebraska and Indiana. These states are all faced with the challenge of making immunization data available to consumers. Each needed to decide if changes would be made to the WIR software or if workflow changes would be made to access the data.

As a solution to remove the barrier of keeping immunization records up-to-date, **Nebraska** rolled out a statewide immunization registry in 2008. The Nebraska State Immunization Information system, NESIIS, was developed to collect and share immunization records among providers, public health, schools and hospitals. This web based application stores immunization information for children and adults in Nebraska.

Currently there are over 1.7 million patient records in NESIIS, and approximately 9 million immunization events. Nebraska's population of approximately 2.4 million is serviced by 1,800

organizations that provide immunizations. NESIIS interfaces with the vital and death records system in the state and all newborns are added to the system. NESIIS helps to service the public health goal of preventing the spread of vaccine preventable diseases. A major barrier to reaching this goal is the continuing difficulty of keeping immunization records accurate and up-to-date. It is difficult for providers and parents to accurately assess the immunization status of their children and patients when records are scattered between medical provider offices and parent records. NESIIS can help eliminate missed opportunities and over-immunization by providing one secure location to store complete immunization records.

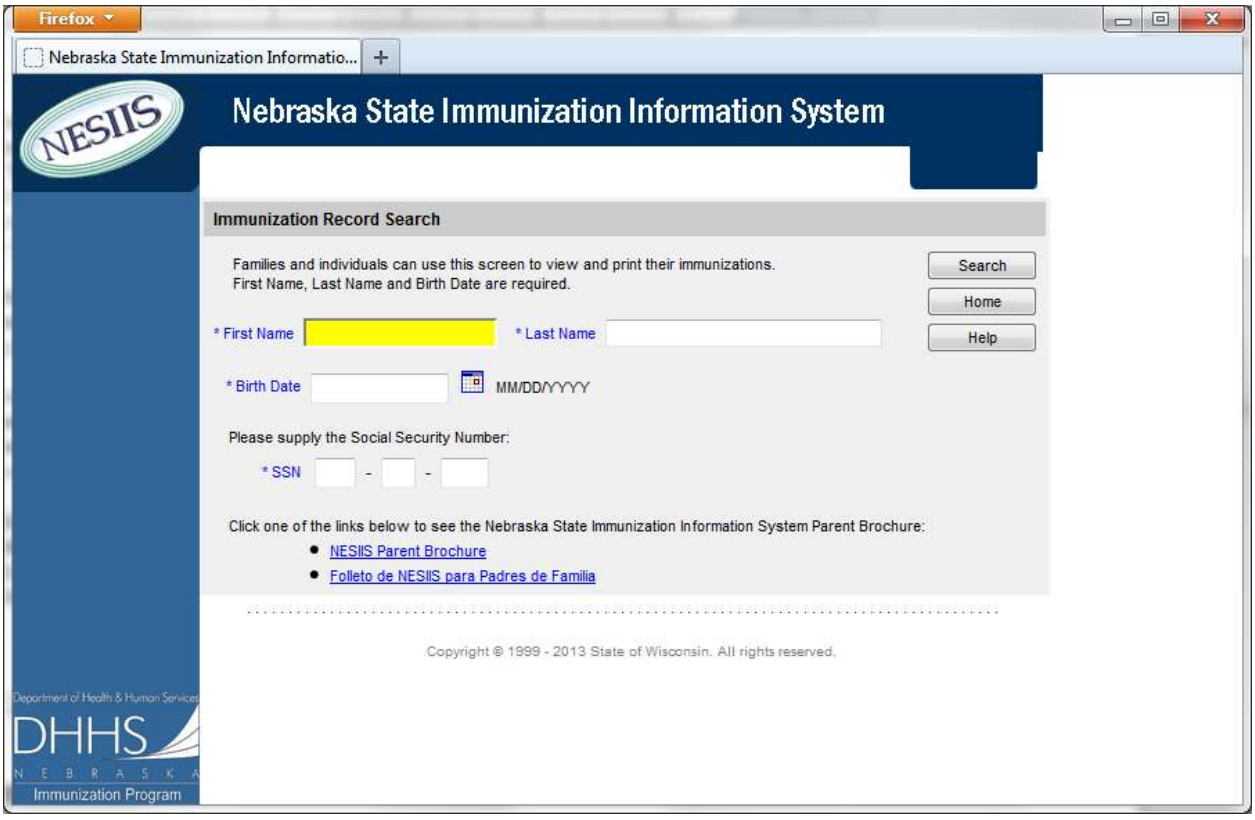

Figure 1 – NESIIS Public Access Screen

Nebraska provides consumer access through a state website (see Figure 1). This information is provided to the consumer by their provider or the DPH help desk. Signup for web access to immunization data is relatively easy. The search criteria are based on SSN, first, last name and date of birth. A query is sent to NESIIS and immunization history and forecast are returned. No protected health information (PHI) or provider locations from immunization events are returned. An official immunization record can be printed and provided to a school, camp or day care center. Most schools, however, access NESIIS directly.

Mobile application has not been requested. Individuals can access the web site via their smart phone. This application has been used as a proof of age verification for parents that are traveling with children during an airport security check.

Wisconsin IIS manager Tom Maerz met with HLN to discuss the work happening with the Wisconsin Immunization Record (WIR) and how they are addressing public access. In 2005, as part

of the Governor's Kid First Initiative, focus was placed on targeting immunization efforts to areas where numbers of children immunized was low.

Wisconsin has 7.7 million clients and 69 million immunizations to date. Today there are over 35,000 consumer accesses per month to the WIR system and during the peak time in August the system sees upward of 54,000 accesses. When Wisconsin was making the decision to roll out public access they were looking to find search criteria that would authenticate the user and be easily supported. They were concerned about the support impact of using a registry-provided PIN to consumers (see Indiana approach below).

Figure 2 – WIR Public Access Screen

When initially established, WIR used SSN and Medicaid ID along with name and date of birth as the key search criteria. At that time, Medicaid ID was the most used search key and there were approximately 7,000 accesses per month. By 2009, SSN had become the key patient identifier used by consumers to locate records. Recently, after attending an ONC Consumer Access meeting, the Governor charged his staff with deploying search by medical record number (both clinical and HMO). This has been a popular addition to the system. It was noted that parents often forget their

children's SSN but always have a copy of their insurance card. Wisconsin is the first state to employ this enhancement in the WIR system.

Access to WIR is via the same web portal used by providers except individuals click on "public access" (see Figure 2). The searching is more restrictive than the provider search and requires an exact match for information to be returned. The information provided is a confidential immunization record with history and forecast. No provider or protected health information is visible. This information can be printed and is accepted as an Official Record for schools and camps. The application is available in English, Spanish, and Hmong.

Indiana deployed the Children and Hoosier Immunization Registry Program (CHIRP) to address the need to provide a consolidated immunization record. This information was made available to the public through their provider. With encouragement from the ONC and funding from the Health Information Technology for Economic and Clinical Health (HITECH) fund, Indiana developed a business model to provide public access to immunization data. They concluded that access to the data should be through a secondary portal. In July 2012 they announced the "MyVAXIndiana" web portal to allow individuals direct access to their immunization records.

Individuals receive authorization and a PIN number from their provider – the PIN is a randomly-generated five to ten digit number with no inherent meaning. This method of authentication was selected because of the strong patient-provider relationship and since most of the requests come through the providers. In addition, providers found that it took less time to provide access to their patients than to print the immunization summary report themselves. Indiana has 5.8 million patients and just over 50 million vaccinations in CHIRP. Currently there are over 34,000 people registered for the MyVaxIndiana portal.

The provider can print off the PIN number or send it to the patient via e-mail. E-mail is recommended because it can be easily retrieved or resent if the patient loses the PIN. If the provider has an HL7 interface, they can send the request for patient access to CHIRP (including the patient's email address) using that capability and the PIN and URL are sent to the patient's e-mail by CHIRP. They are investigating allowing a PHR vendor to also submit patient registration requests (but not provide direct access to data through the PHR). Some providers resist participation because they are not comfortable with patients having access. If this situation arises, the patient is directed to the help desk for assistance. The state law states that individuals have a right to their records. This is something that they stress to providers.

Figure 3 – MyVaxIndiana Public Access Screen

Along with the PIN number the individual must know the first and last name and the DOB (see Figure 3). An additional security question is presented and needs to be typed to prevent bots from attacking. Individuals can print out 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. This is located on the screen but is represented in orange instead of blue. Consumers have asked for a mobile version. This was rolled out recently and in one month there were over 1,000 downloads.

4.1 Snapshot of Three States Interviewed

The following table summarizes the consumer access projects in the three aforementioned states interviewed:

	Nebraska	Wisconsin	Indiana
Registry Name	NESIIS (WIR implementation)	WIR	CHIRP
Consumer Access	• Started on 2010 • Via state portal. Separate web application against production IZ database	• Started in 2005 when Governor announced Kids First • Same web portal as provider link • More restrictive search then providers	• Access via MyVax Indiana • Patients need URL and PIN from provider or help desk
State Laws	• Wrote original statutes but they need updating	• None on public access	• State law says individual has the right to see their record
Search Criteria/Identifiers	• SSN used as unique identifier but not mandatory • Also need name DOB	• First released with SSN or Medicaid ID Recently added MRN. Very popular search • Also need name, DOB	• PIN required • Also need name and DOB
What you see	• Print official record • No SSN, physician's name or location of IZ displayed • Access to proof of age by children • Schools have separate access	• Print official record • Provides history and forecast info • No location for shots or providers • Provide only PHI that was already provided	• Print official record • No SSN, physician's name or location of IZ given
Functionality	Print only	Print only	Print, possibly more

5 Models for IIS Consumer Access

Deloitte's partner, HLN, examined all available material and developed the following set of options for IIS consumer access relevant to the WIR software that is in use. This is a somewhat complex set of choices – some options are variations of others. All options do not meet the requirements defined in Section 3 above equally; exceptions are noted below. Additional discussion about the relative merits of these options can be found in the Conclusions and Recommendations section below. It is important to note that in many cases the options are not mutually-exclusive: multiple strategies can be pursued simultaneously.

The following diagram depicts the relationship of these options to one another:

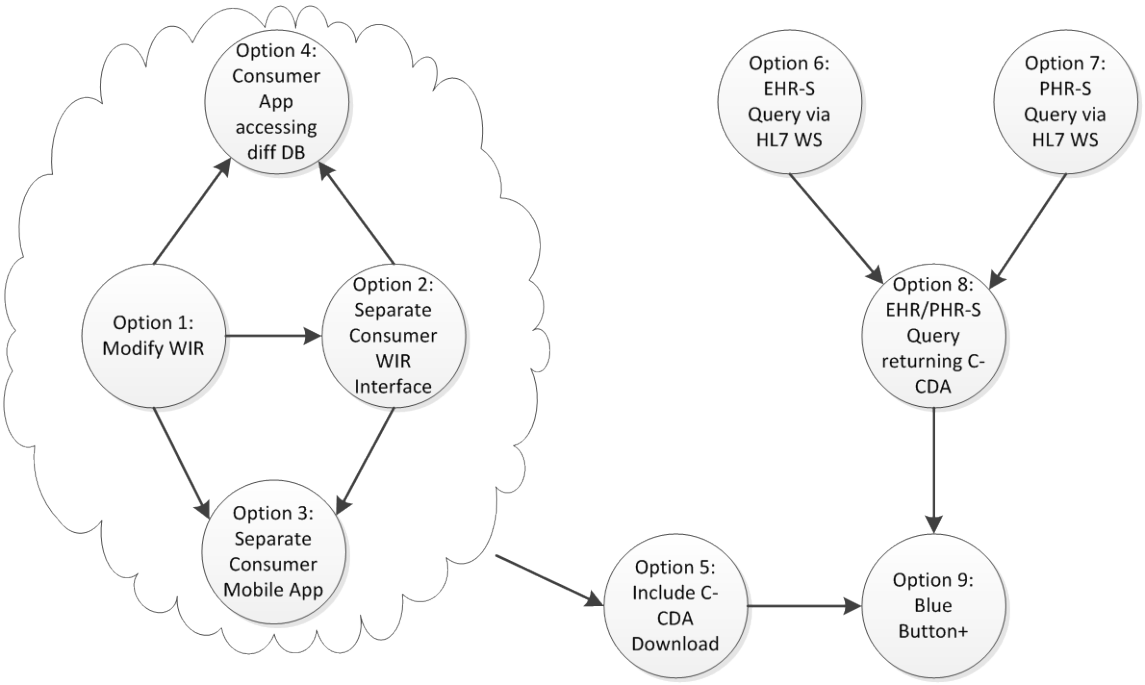

Figure 4 – Consumer Access Options

The following table describes each option, its strengths, and challenges:

Option	Strengths	Challenges
1. Modify software to provide a new web-based user interface for consumer access. This new interface accesses the same underlying database as the IIS provider client. Users can be authorized by IIS staff, primary care provider, or no one at all (user must substantiate relationship with patient through knowledge of	• Allows the IIS to retain control over the user "experience" • IIS branding can be prominent throughout the user's interaction • Common base of data maintained through access to primary IIS database • Various methods of user authentication and authorization possible • Display, report generation, and	• Patients will only be able to access information in the IIS database, no more, no less • As usage increases, performance of IIS database may be negatively affected • May require "negotiation" with State IT over firewall and other security settings and restrictions for consumer access

Option	Strengths	Challenges
patient demographic details). Users should be able to view a record and download a PDF of the record at minimum.	data download options can be mixed and matched, and phased in over time • Allows for leveraging of software development with other states if they share the software (*e.g.,* WIR) • Easier to impose two-factor authentication • Potential exposure of PHI in consumers hands limited to immunization data and minimal demographics	• User authentication and authorization may be challenging to implement and support • If required, two-factor authentication of users may be challenging and expensive to support • Authorization for access based solely on user knowledge of patient demographics may provide insufficient audit trail for system access • Cost of software modifications may be significant • Does not leverage emerging PHR market • Not consistent with growing ONC-inspired Blue Button architecture • Users of provider portal may become confused and try to access the IIS using consumer portal instead
2. Rather than modifying the IIS software itself, create a new, separate, stand-alone web-based interface for consumer access (variation on Option 1).	• Allows the IIS to retain control over the user "experience" • IIS branding is prominent throughout the user's interaction • Allows for leveraging of other states if they share the software (*e.g.,* WIR) • May be easier for State IT's to secure a more separate application • Various methods of user authentication and authorization possible • Display, report generation, and data download options can be mixed and matched, and phased in over time • Easier to impose two-factor authentication	• As usage increases, performance of IIS database may be negatively affected • User authentication and authorization may be challenging to implement and support • If required, two-factor authentication of users may be challenging and expensive to support • Does not leverage emerging PHR market • Not consistent with growing ONC-inspired Blue Button architecture
3. Create a mobile app to supplement or replace a web-based app for consumer access	• Appeals to current trend in individual computing • Reduces barriers to using	• May involve new skill sets for PHA and/or its technical contractors

Option	Strengths	Challenges
(variation on Options 1 & 2)	application by consumers • Applications tend to be easy to use and intuitive • Easier to impose two-factor authentication	• May provide limited capabilities for printing reports • May require multiple applications for multiple platforms (*e.g.,* iPhone and Android)
4. Modify IIS or create a new module to provide consumer access relying on data from a separate immunization data store (variation on Options 1 & 2)	• Allows IIS to retain control over the user "experience" • IIS branding is prominent throughout the user's interaction • Potential IIS database performance impact averted through separate database optimized for consumer query • Allows for leveraging of other states if they share the software (*e.g.,* WIR) • • Enhanced security due to more limited data set in consumer access database • Potential to provide consumer access to other data unrelated to IIS , including general-purpose health information (*i.e.,* not patient specific but context specific) • May be easier for State ITs to secure the application due to its more focused audience and more limited data • Various methods of user authentication and authorization possible • Display, report generation, and data download options can be mixed and matched, and phased in over time	• Additional effort and cost required to create separate database and synchronize continuously with primary WIR based database. • User authentication and authorization may be challenging to implement and support • If required, two-factor authentication of users may be challenging and expensive to support • Does not leverage emerging PHR market • Not consistent with growing ONC-inspired Blue Button architecture
5. Through a direct web-based user interface, allow patients to download a C-CDA file with the immunization record and forecast (Blue Button; variation on Options 1, 2 3 or 4).	• Same as Option 1, 2, or 3 • C-CDA more consistent with emerging national standards • Leverages CMS MU activities and expectations • Step in the right direction towards Blue Button+ • Easier to impose two-factor	• Clinical documents (C-CDA) represent new territory for most public health agencies; limited training and experience

Option	Strengths	Challenges
	authentication	
6. Allow EHR systems to query IIS for patient records and forecast via HL7 v2 messages. Encourage patient access through interfaces provided by provider organizations.	• No modifications to IIS required • Leverages current national interoperability standards, including likely MU Stage 3 requirements • Pushes burden of patient authentication and authorization onto provider organizations which have preexisting relationship with the patient • Consistent with MU requirements for View/Download/Transmit of patient records • Encourages provider query of IIS and incorporation of more complete records into EHR systems • Provides easy to fulfill "carrot" for patients to provider-based systems for records access • Can easily be expanded to incorporate Option 5 simultaneously	• IIS loses much control over the user's "experience" including what data is provided and in what format. • Dependent on providers' implementation of HL7 query and proper processing of responses. • As query usage increases, performance of IIS may be negatively affected • Current "read-only" CCOW-enabled EHR query of IIS cannot use this functionality • Harder to impose two-factor authentication • Some patients may not have routine access to a primary care provider and thus might not have access to the data • Potential exposure of PHI in patients hands may be increased as immunization data may be combined with more sensitive health information
7. Allow authorized PHR systems or HIE to query IIS for patient records and forecast via HL7 v2 messages. Patient access is the provided through PHR account. IIS relies on PHR to authenticate and authorize users.	• Same as Option 6 • Can coexist with Option 6 • Expands access to consumers by providing another channel in addition to provider-enabled systems • Opens up the potential for patients to consolidate patient records from multiple sources, and for authoritative immunization data to be included	• Same as Option 6 • Requires extension of trust domain to PHR systems which may require new or different data sharing agreements and use of legal services • Penetration and use of PHR systems may continue on a slow pace yielding limited consumer access to data especially in the short run • Harder to impose two-factor authentication • Potential exposure of PHI in patients hands may be increased as immunization data may be combined with more sensitive health information
8. Allow EHR and/or PHR	• Consistent with Options 6 and 7	• Same as Options 6 and 7

Option	Strengths	Challenges
systems and/or HIE to query IIS for patient records and forecast via HL7 v2 messages, but return a C-CDA document	• More consistent with emerging format for electronic medical records interoperability • Can be implemented independent of current IIS software through web services (*i.e.,* new web service intercepts EHR/PHR query, sends query on to IIS, receives data and converts to C-CDA)	• Clinical documents (C-CDA) represent new territory for most public health agencies; limited training and experience • Harder to impose two-factor authentication
9. Implement Blue Button+, which allows patients to "subscribe" to records in IIS and have an updated immunization history and forecast in C-CDA format "pushed" to the participating PHR of their choice via Direct e-mail.	• Consistent with emerging model for consumer access to electronic medical records • Pushes burden of patient authentication and authorization onto provider organizations which have preexisting relationship with the patient	• Requires a whole new set of technologies to be implemented (C-CDA, Direct, publish/subscribe), and associated costs may be significant • Need to determine which events trigger "push" of updated data since forecast can change simply with the passage of time • Requires extension of trust domain to PHR systems which may require new or different data sharing agreements and use of legal services • Current PHR systems may have limited ability to support BB+ yielding limited consumer access to data especially in the short run • Harder (if not impossible) to impose two-factor authentication

6 Authentication and Authorization of Consumers

High on the list of challenges for consumer access to data is proper authentication and authorization of users. Authentication is the process of validating that the person trying to access data is who they say they are. Authorization is the process of determining that the authenticated user has the right to view the data being requested. These are separate, but inter-related issues. Authentication is a common event and one that consumers encounter it every day. In the banking industry you are provided a bank card and a PIN number to access your account electronically.

Authentication usually starts with some method for confirming the identity of a user before assigning that user credentials to access a system. This step is often called "identity proofing" and can involve everything from face-to-face authentication by someone authorized to perform this function (a system administrator, or even a provider if providers are assigned a "gatekeeper" role on behalf of their patients) to merely challenging the new user with a set of questions whose answers you hope only that user knows. Once a user's identity is validated they are assigned credentials – usually this is just a username and password that only they are supposed to know – which are used to authenticate a user when they try to access the system. This type of authentication is referred to as "single factor authentication" because it involves only one kind of method: username and password. When a user is assigned a username and password for authentication, the system is also told *what* data the user is permitted to access (might be some, might be all), which represents the user's *authorization* to access resources.

Some types of data access require a more secure set of credentials. When a second level of authentication is introduced – like an additional one-time password that is specially generated in real time for each transaction, a digital certificate, or a biometric like a retinal scan or thumb print – the transaction is considered more secured since users must not only present something they *know* (initial username/password) but also something they *have* (like a digital certificate) or something they *are* (like a biometric). These types of authentication – referred to as two-factor authentication – are much harder (and in some cases impossible) to forge.

The following table details options that are available for authenticating and authorizing consumer access to IIS data. Individual projects need to weigh the strengths and weaknesses of each option and examine them within the constraints and requirements of their larger organization's security policy:

Option	Strengths	Challenges
1. No specific authentication other than knowledge of enough data to successfully query and return a single result. Data might include: a. First name b. Last name c. Data of birth d. Gender (no known sites using this method)	• Very little burden on PHA or provider	• May provide too many opportunities for inappropriate data access since relationship to the patient is not verified • No identity proofing of the user • Little or no useful auditing of user access possible

Option	Strengths	Challenges
2. No specific authentication other than knowledge of enough data to successfully query and return a single result (similar to Option 1 above) *including* at least one unique identifier which might be: a. Social Security Number b. Medical Record Number c. Medicaid ID (*e.g.,* WIR, NESIIS)	• Little burden on PHA or provider • Reduces risk of inappropriate data access through corroborating data that unauthorized individuals typically do not know	• Requires corroborating unique identifier to be stored in the IIS • Requires method for missing or incorrect unique identifiers to be updated/corrected in IIS • No identity proofing of the user • Little or no useful auditing of user access possible
3. User can only access record with a PIN number associated with the patient provided by the IIS through a primary care provider or PHA site. PIN is either provided on paper or via e-mail along with the access site URL. (*e.g.,* Indiana CHIRP)	• Ensures that access is provided only to individuals personally known to a provider or PHA or whose identity and relationship to the patient can be verified • Auditing of user access provides specific information about who accessed patient records	• Adds burden on PHA or provider to distribute PIN, though this may be less effort than actually providing the immunization data • Add burden to provide lost PINs again, though this may be mitigated somewhat by sending PIN via e-mail which can be retained by the recipient
4. User identity established through rigorous identity-proofing (may require in-person validation or automated validation through the use of third-party verification services). Access requires two-factor authentication (username/password as well as a one-time password provided via e-mail or text message, or use of third-party verification services). (no known sites using this method)	• Ensures that access is provided only to individuals personally known to a provider or PHA or whose identity can be verified • Access of records required authentication consistent with National Institute of Standards and Technology (NIST) Level 3 • Auditing of user access provides specific information about who accessed patient records	• Difficult part is establishing relationship to the patient (authorization to access specific records), not authentication of the user (in other words, strong authentication without authorization does not appear to accomplish much) • May require coordination, leverage, or reliance on broader PHA state consumer authentication initiative • Cost to implement and support this option higher than other options • This option does not appear to offer protection superior to Option 3

7 Conclusions and Recommendations

After reviewing the research conducted for this project, the Deloitte and HLN team offers the following conclusions and recommendations:

- Unless outreach into the community has been done to determine if this functionality is desired or demanded, significant investment in a consumer access strategy should be limited until a purposeful engagement with consumers or consumer advocate organizations takes place.
- States that have provided consumer access have done so with little up-front cost and little to no impact on current IIS operations or system performance.
- The EHR market is not yet very sophisticated in terms of patient access, but the impending implementation of MU Stage 2's "view/download/transmit" measure may quickly change this. Dominance of a particular EHR system vendor in a given market could provide some leverage in that particular space. State and local public health agencies (PHA) may provide a point of access for patients without a medical home.
- State and public health agency technical, legal, and information security staff members should be fairly involved in IIS operations and decision-making so any move toward providing consumer access will require the scrutiny of these offices. This may limit IIS' ability to move forward quickly or easily.
- If there is no unique identifiers in the IIS known easily to the outside community (Social Security Number (SSN), Medicaid ID, Medical Record Number (MRN)), consumer access cannot be provided without some level of effort, technical or administrative. Note: Indiana's PIN access was not achieved using WIR software.
- User identity proofing issues for consumer access are somewhat of a red herring: The tough part is not independent user authentication but rather user *authorization*, *i.e.,* establishing the user's relationship to the patient. This is difficult to do in an IIS alone without corroborating that relationship with data in the IIS or validating that independently with another source (like the provider).
- In terms of the implementation options identified in the report, it may be challenging for a PHA to expand the use of the WIR software web client for consumer access. Creation of a mobile app is probably the most forward-thinking in terms of consumer access and emerging technology usage patterns, though the difficulty in printing a formatted report from a mobile device may be a real barrier. Permitted access via query from electronic health record (EHR) and/or personal health record (PHR) systems require the least modification to operations and software, but require close cooperation with the vendors and sites. Pursuit of a Blue Button+ strategy allowing patients to "subscribe" to records in IIS is the most forward-thinking of all the options.

8 Appendix A: Sources

Ancker, Jessica S et al. "Consumer experience with and attitudes toward health information technology: a nationwide survey." *J Am Med Inform Assoc* 2013; 20:152-156.

Fridsma, Doug. "Automate Blue Button Initiative (ABBI) Status update." Health IT Standards Committee Update. November 13, 2012.

Morris, Genevieve et al. "Consumer Engagement in Health Information Exchange." Audacious Inquiry (for ONC), September 30, 2012.

Morris, Genevieve et al. "Key Considerations for HIOs Supporting Stage 2 Patient Electronic Access." Audacious Inquiry (for ONC), July 5, 2013.

ONC State Health Policy Consortium Project. "Consumer Innovation Challenge: Final Report." RTI International, February 2013.

Ozbolt, Judy et al. "Summary Report of Consumer eHealth Unintended Consequences Work Group Activities." Westat: September 19. 2012.

Siminerio, Erin Poetter et al. Webinar: "Introducing Blue Button Plus An Implementation Guide for Developers and Data Holders." National eHealth Collaborative (NeHC). February 19, 2013.

Webinar: "An Introduction to The Consumer Consortium on eHealth." National eHealth Collaborative (NeHC). February 19, 2013.

ONC State Health Information Exchange Program, "State HIE Bright Spots Synthesis, Public Health Part 1: Improving Individual Access to Immunization Records," March 2012 (unpublished).

9 Appendix B: Glossary of Terms

BB+	Blue Button+
CDC	Centers for Disease Control and Prevention
CHIRP	Children and Hoosier Immunization Registry Program
CMS	Centers for Medicare & Medicaid Services
EHR	Electronic Health Record
EP	Eligible Professional
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
IIS	Immunization Information System
MRN	Medical Record Number
MU	Meaningful Use
NCIRD	National Center for Immunization and Respiratory Diseases
ONC	Office of the National Coordinator for Health Information Technology
PHA	Public Health Agency
PHI	Protected Health Information
PIN	Personal Identification Number
PHR	Personal Health Record
SSN	Social Security Number
S&I	Standards and Interoperability Framework
VA	U.S. Department of Veterans Affairs
WIR	Wisconsin Immunization Registry