FOCUS PATIENT ENGAGEMENT

Consumer Access to Immunization Information Systems

Public Health and Patient Empowerment

By Noam H. Arzt, PhD, FHIMSS; Emily Emerson; Sripriya Rajamani, MBBS, PhD, MPH; and Katie McGee

ABSTRACT

Consumer access to health information including immunizations is a priority driven by Centers for Medicare and Medicaid Services EHR Incentive Programs and other federal consumer health data initiatives. Understanding legal and technical nuances of granting consumer access to individual health information in public health environments is essential given the emphasis on consumer/patient engagement at both local and national levels.

For more than 20 years, states and other jurisdictions have been collecting data about immunizations for their population in an Immunization Information System (IIS), or immunization registry. Granting access to these data for consumers in a public health context can present with both unique opportunities, and challenges.

This article will describe an approach taken by Minnesota's IIS, the Minnesota Immunization Information Connection (MIIC). The study team conducted interviews and an environmental assessment was done to understand approaches by other states and to determine how various federal and state organizations and vendors are addressing consumer access to immunization information and related challenges of access control.

The study resulted in a set of requirements, options, and limitations for providing consumers access to their immunization information. The options developed can be used by other IISs to engage their stakeholders in determining whether consumer access is warranted and feasible. The findings from this study are being used for another project, a collaborative approach across some states that share the same IIS software to determine best practice approaches for consumer access to data and use this as a model for public health role in patient engagement.

KEYWORDS

Patient engagement, consumer access, access to immunization information system, public health, access options, opportunities and challenges for access, strategy for sustainability.

FOR MORE than 20 years, states and other jurisdictions have been collecting data about immunizations for the population in a state or locally-based common, shared database originally referred to as an immunization registry but more commonly referred to as an Immunization Information System (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] The Minnesota Immunization Information Connection (MIIC) has been in use for ten years. It is based on the Wisconsin Immunization Registry (WIR) software application that is used (in one form or another) by nearly 20 IISs in the United States.

Individual/consumer access to these IISs has recently been identified as a priority initiative of the Office of the National Coordinator for Health Information Technology (ONC), the CDC and state immunization programs. This initiative is part of a large federal initiative related to consumer access to data that includes more than just healthcare.[2] However, there are a number of legal and technical challenges to overcome to allow individual access to MIIC data. Minnesota is investigating the opportunity for consumer access to their immunization information system data in support of federal consumer health data initiatives.

In January 2013, MIIC had nearly 6.5 million clients and more than 58 million immunizations in its database. MIIC is a web-based system that provides documentation and access to information about immunization records for Minnesota residents and Minnesota patients from other states who receive care in Minnesota. Minnesota has a population of approximately 5.4 million people; MIIC holds more clients than state population due to data from neighboring state residents receiving care in Minnesota. Providers can submit data to the system through several methods. These include hand entry through the web-based client, through HL7 standard messaging, through a flat file batch process or through a flu vaccine spreadsheet. MIIC collects data about immunizations and offers providers an immunization history and forecast for each patient. The forecast offers recommendations to assist providers in administering immunizations. Provider information on enrolling in MIIC, the user agreement document, information on how to submit and exchange data, plus training and support materials can be found on the MIIC web page.[3]

Currently, no particular legislation addresses consumer access to immunization information in Minnesota. The Minnesota Immunization Data Sharing law, Minnesota Statutes §144.3351, protects patients' right to privacy and states that the only person who can see an individual's immunization records must either be someone who administers immunizations, a person who provides immunization services on behalf of the patient, or someone who is required by law to record immunizations for enrollment—a patient's provider, public health agencies, schools, daycare centers or insurance companies.[4]

PROJECT METHODOLOGY

Minnesota was seeking options and strategies for consumer access to immunization information in response to a top down initiative that the White House has launched to provide consumers with direct access to their health records. To this end, the project team – made up of Minnesota Department of Health (MDH) staff and outside consultants – performed a series of interviews and conducted research to determine what other states are doing to fulfill this need for their constituencies. The interviews spanned individuals and organizations in state and federal government, as well as other key stakeholders in Minnesota. The research and interviews were designed to paint a broad brushstroke of the legal, technical and policy issues surrounding access to MIIC. The goal of the research 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. The team did not focus on the consumer desire for this technology and did not conduct user group sessions or focus groups to provide this background.

ENVIRONMENT ASSESSMENT

Federal Perspective. ONC is looking at many different strategies to address consumer access to healthcare data. While the original release of HIPAA in 1996 guaranteed the right of access to personal healthcare information, access to these data still presents many technologic challenges and consumer demand is marginal. CMS' EHR Incentive Program's Meaningful Use (MU) encourages enhanced patient engagement and consumer access. ONC posted a web page seeking the public's input on Federal Consumer eHealth Strategies. This page details the ONC's "3 A's" of consumer engagement: Access, Action and Attitude.[5] It notes that when patients have the ability to review and update their health record, they then become active participants in their healthcare. A recent survey stated that 60 percent of people interviewed would consider changing their healthcare provider if they could access their healthcare records.[6] Immunization data may be relevant to this finding.

One of the solutions to providing 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.[7] The application was developed to allow veterans to easily access and download their medical data for their own use or to share with other medical providers.[8] In 2013 ONC released Blue Button+ (BB+), which extended the original Blue Button initiative.[9] 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 marketplace to determine how and what types of tools should be developed.

The CMS EHR Incentive Programs provide another backdrop for consumer access to health data including immunization

TABLE 1: Relevant Minnesota Laws and Statutes

	Health Records and Reports[1]	Description
144.29	Health Records; Children of School Age	Requires schools to keep health records and that these must be easily transferred so as to follow the child to other schools. Data Classified as "private" per Minn. Stat. 13.05. Generally requires appropriate safeguard procedures for storage and disposal when no longer needed.
MINNESOTA HEALTH RECORDS ACT		
144.291	Minnesota Health Records Act	Defines the players and kind of information i.e., who are providers; what is a Health Information Exchange; what constitutes a health record; etc.
144.292	Patient Rights	Provides information on a patient's right to health records; what must be given, when and for how much and to whom the info may be given.
144.293	Release or Disclosure of Health Records	Gives information on consent and exceptions to consent requirements for release of health records.
144.294	Records Relating to Mental Health	Provides guidelines on whom the records can be released and under what circumstances.
144.295	Disclosure of Health Records for External Research	Describes methods of release and duties of the researcher.
144.334	Right to Request Patient Information	Requires the provider to request the patient's authorization to release information about the patient to a designated individual.
144.3351	Immunization Data Sharing	Provides information on who can share immunization data without consent and what data can be shared.
HEALTH AND MEDICAL DATA		
13.3805	Public Health Data	Provides information on disclosures among or between providers and public health as needed, to locate or identify a case, carrier or suspect case for purposes of diagnosis, treatment and epidemiologic investigations.

data.[10] 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 EHR systems and their "meaningful use". This multiyear program is rolling 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, that eligible professionals and hospitals will be expected to support if the public health agencies in their jurisdictions are capable of exchanging data electronically. While immunization reporting is a "menu set," or optional measure in Stage 1 of the program, it 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."[11] "View/Download/Transmit" represents a new, more formal requirement for patients to access their own health data through the provider's EHR system. Blue Button/Blue Button+ may become one strategy for providing this access. As Minnesota contemplates strategies for providing access to MIIC data directly to consumers, these initiatives may provide guidance in accomplishing this goal.

National IIS policy originates with the National Center for Immunization and Respiratory Diseases (NCIRD), a branch of the CDC. From the CDC perspective, the biggest concern for the IIS programs is the lack of tools to ensure identity proofing of consumers (see next section). 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.

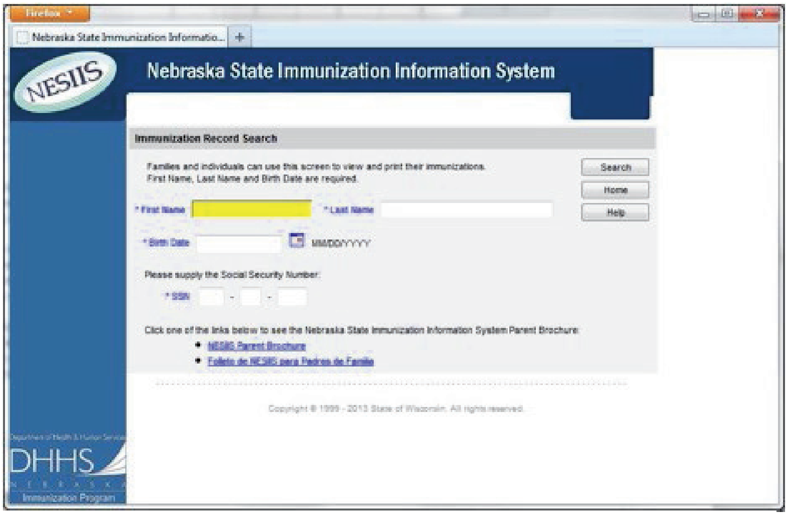
Minnesota State Perspective. Minnesota has various statutes addressing data privacy, health records and reports for schools. The project team did not do an exhaustive search of all laws and statutes in Minnesota, but the cursory review indicated there were no specific laws, statutes or rules on record that address direct consumer access to immunization data. Much of the information described next makes reference to access of healthcare records and refers to paper charts rather than electronic access.

In addition, the MDH website provides instructions on how citizens can obtain their health records, which include immunizations.[12]

The overarching challenge within MDH is how to provide services to their client base while balancing the cost of operations and completing priorities as state government IT services have been centralized. Currently, parents in Minnesota can call the MIIC help desk to get immunization data for their children younger than age 18. Parents must be able to provide certain information to be authenticated. However, this is not direct consumer access to MIIC. One key challenge is that MIIC cannot store certain identifying information like social security number (SSN). Therefore, it is challenging to set up a method to authenticate users. The new Health Insurance Exchange (HIX) might be a viable option. This would mean that the federal government would provide the authentication and allow Minnesota to build the access tool. Currently there are no other initiatives in Minnesota for statewide user authentication.

When considering direct patient access to MIIC, these options may need to be legislatively authorized. At a minimum, the MDH legal department would need to weigh in on any data-sharing agreements that are developed. Currently, the only access to state databases is for aggregate data. The MDH website discusses (but does not provide) access to vital statistics data per Minnesota Statutes, §144.225, subdivision 7, which limits access to a birth or death certificate to a person who has tangible interest. The "tangible interest" requirement helps protect people who are born in Minnesota and the families of people who have died in Minnesota against fraud and identity theft."[13] While MDH continues to discuss online ordering from the vital statistic website, it recognizes that identify theft as the fastest growing type of crime in the United States. So far, MDH has not yet determined how to ensure that only someone with tangible interest is making an online request. Additionally, statutory changes will be required to provide this type of access.

FIGURE 1: NESIIS Public Access Screen


Firefox
Nebraska State Immunization Informatio...
+
NESIIS
Search
Home
Help
Department of Health & Human Services
DHHS
NEBRASKA
Immunization Program

Nebraska State Immunization Information System

Immunization Record Search

Families and individuals can use this screen to view and print their immunizations.
First Name, Last Name and Birth Date are required.

* First Name * Last Name

* Birth Date MM/DD/YYYY

Please supply the Social Security Number:

* SSN - -

Click one of the links below to see the Nebraska State Immunization Information System Parent Brochure:

- NESIIS Parent Brochure
- Folleto de NESIIS para Padres de Familia

Copyright © 1999 - 2013 State of Wisconsin. All rights reserved.

CURRENT CONSUMER ACCESS TO IIS IN THE U.S.

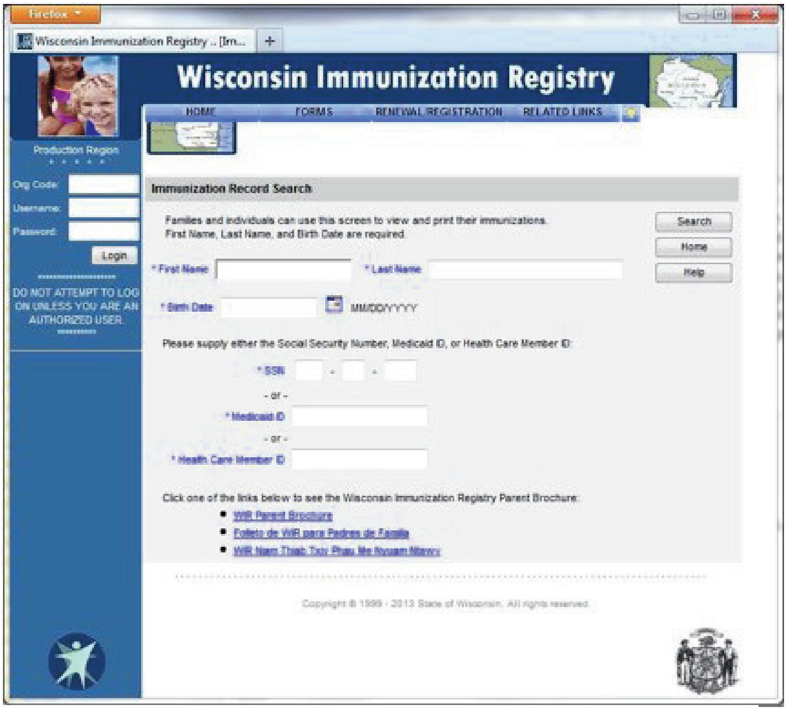
Interviews were held with three states currently providing consumer access to their IIS data: Wisconsin, Nebraska and Indiana. These states were faced with the challenge of making immunization data available to consumers. Each state needed to decide if changes would be made to their IIS software or if workflow changes would be made to access the data.

As a solution to removing 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. Nebraska provides consumer access through a state website (see **Figure 1**). This information is provided to consumers by their provider or the Nebraska Department of Public Health's 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 daycare center. Most schools, however, access NESIIS directly. Mobile application has not been requested. Individuals can access the website via their smart phone. This application has been used as a proof of age verification for parents who are traveling with children during an airport security check.

In 2005, as part of the Governor's Kid First Initiative, Wisconsin targeted immunization outreach efforts to areas where children were under-immunized. By the spring 2013, there were over 35,000 consumer accesses per month to the WIR system, and during the peak time in August, the system saw upward of 54,000 accesses. When Wisconsin was making the decision to roll out public access, they looked for search criteria that would also authenticate the user and that could be easily supported. They were concerned about the support impact of using a registry-provided PIN number to consumers (see Indiana approach next).

When consumer access was 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 health maintenance organization, 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 Official Records for schools and camps. The application is available in English, Spanish and Hmong.

FIGURE 2: WIR Public Access Screen



Wisconsin Immunization Registry

Immunization Record Search

Families and individuals can use this screen to view and print their immunizations.
First Name, Last Name, and Birth Date are required.

* First Name: * Last Name:

* Birth Date: MM/DD/YYYY

Please supply either the Social Security Number, Medicaid ID, or Health Care Member ID:

* SSN - -

- or -

* Medicaid ID

- or -

* Health Care Member ID

Click one of the links below to see the Wisconsin Immunization Registry Parent Brochure:

- WIR Parent Brochure
- Folleto de WIR para Padres de Familia
- WIR Nam Thab Txiv Phau Me Nyuam Ntawv

Copyright © 1999 - 2013 State of Wisconsin. All rights reserved.

DO NOT ATTEMPT TO LOG ON UNLESS YOU ARE AN AUTHORIZED USER.

Indiana deployed CHIRP, Children and Hoosier Immunization Registry Program, to consumers 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 HITECH fund, Indiana developed a business model to provider 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. By spring 2013, there were over 34,000 people registered for the MyVAX-Indiana portal.

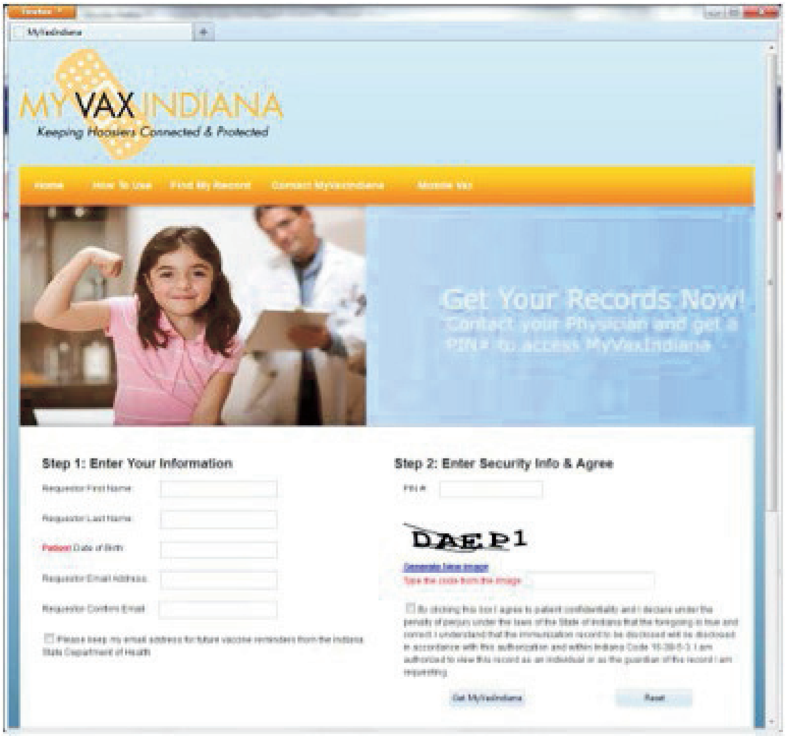
The provider can print off the PIN number or send it to the patient via e-mail. E-mail is recommended because it can be easily retrieved or resent if the patient loses the PIN. If providers have an HL7 interface, they can send the request for patient access to CHIRP (including the patient's e-mail address) 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 CHIRP help desk for assistance. The Indiana state law states that individuals have a right to their immunization records. This is a fact that CHRIP stresses to healthcare providers.

Along with the PIN number, the individual must know the first and last name and the patient's date of birth (see **Figure 3**). An additional security question is presented and needs to be typed to prevent automated scripts \from attacking the site with phony data requests. 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 asked for a mobile version. This was rolled out recently and in one month there were over 1,000 downloads.

PROJECT REQUIREMENTS

The study team developed the following sets of requirements for consumer access to immunization data from MIIC. These requirements should be used to assess the

FIGURE 3: MyVaxIndiana Public Access Screen



Step 1: Enter Your Information

Requestor First Name

Requestor Last Name

Patient Date of Birth

Requestor Email Address

Requestor Confirm Email

□ Please keep my email address for future vaccine reminders from the Indiana State Department of Health

Step 2: Enter Security Info & Agree

PIN #

Generate New Image

Type the code from the image

□ By clicking this box I agree to patient confidentiality and I declare under the penalty of perjury under the laws of the State of Indiana that the foregoing is true and correct. I understand that the immunization record to be disclosed will be disclosed in accordance with this authorization and within Indiana Code 16-38-5-3. I am authorized to view this record as an individual or as the guardian of the record I am requesting.

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" may be considered optional at this time.

Core Requirements

1. Support for federal consumer health data access initiative as referred to earlier. 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 use MIIC, they can typically enter search criteria that may yield multiple, potential patients to view. Consumers, however, must know enough about a unique record in MIIC 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 (e.g., parent-child) 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 (see previous section on Access Control).

6. User can view consolidated, de-duplicated immunization history (at 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 through the MIIC interface, 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 early childhood program or child care admission. This is a key requirement and is often the reason why parents want access to these data in the first place. Minnesota does not have an official school report, but MIIC's help desk provides a parent report on demand (manually), which is accepted by schools and other programs in the state as a vaccination record. Providers can also produce a slightly different report through MIIC and give it to a parent for presentation to a school or another program.

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 MIIC. Data quality is an ongoing issue to be managed, and enlisting patients in this process can only improve overall data quality. Minnesota needs to consider, however, the resources and funding that might be necessary to follow up on these additional data quality questions, should any surface.

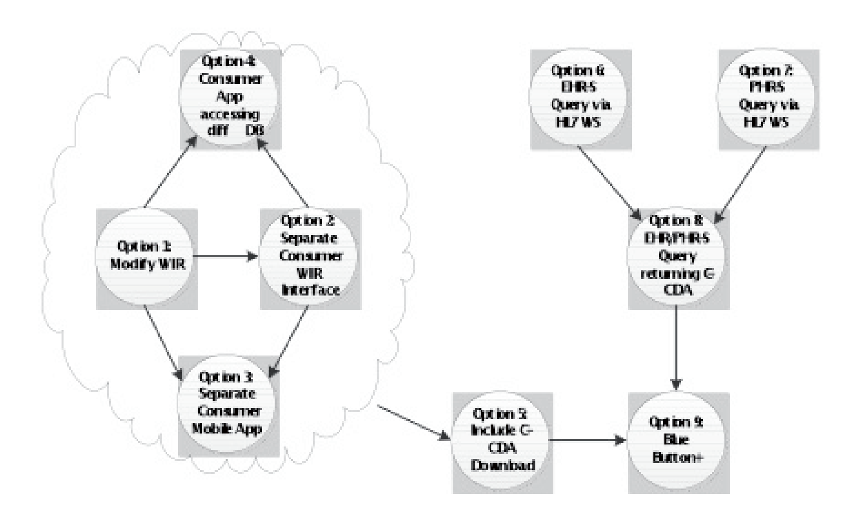
2. Generate reminder/recall notices to "push" to parents electronically. A patient report (see previous core requirement 8) should provide a forecast of immunizations due at the moment the report is generated, but because the forecast changes as the patient ages, it may also be beneficial to "push" a notice in real time from MIIC to a patient or guardian. This must be done securely to ensure that PHI is not transmitted over an unencrypted network or stored unencrypted at an insecure end-point.

Limitations Specific to Minnesota

In addition to the previous requirements, Minnesota has some particular limitations that may also affect viable solutions to this project that must be considered when choosing strategies.

1. No explicit demand from the community for this functionality. As stated earlier in this report, there has been no explicit consumer demand for this access. On the other hand, there has been no consumer education around this potential access, so there may be no basis for consumers to request it. Neither MDH nor the project

FIGURE 4: MIIC Consumer Access Options


Option 4: Consumer App accessing diff DB
Option 6: EHRS Query via HL7 WS
Option 7: PHRS Query via HL7 WS
Option 1: Modify WIR
Option 2: Separate Consumer WIR Interface
Option 8: EHR/PHRS Query returning C-CDA
Option 3: Separate Consumer Mobile App
Option 5: Include C-CDA Download
Option 9: Blue Button+

team made an explicit attempt to engage consumers either directly or through advocacy groups on this issue for this study.

2. Cannot use SSN or Medicaid ID for query. Due to a legal prohibition, MIIC does not contain social security numbers or state Medicaid ID numbers as part of its patient demographics. While use of these unique identifiers would facilitate the return of one and only one record in response to a query (see previous core requirement 3); 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 next leverage MIIC'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 the provider community.

4. Large penetration of Epic with some automated interoperability. In some settings, the Epic electronic health record system has significant penetration and market share. While this may serve as a point of leverage, it may also serve as a point of constraint, as accommodation of Epic in some solutions may produce limitations for other EHR systems.

5. No official Parent Report exists, though the report currently generated from MIIC is widely used. As discussed in core requirement 8, lack of an official report has not been a major impediment to using MIIC-generated data for school or other program entrance, but an official report would certainly provide more leverage for this project.

PROJECT OUTCOMES

Models for IIS Consumer Access. Based on its research, the team developed a set of options for IIS consumer access relevant to MIIC and the WIR software that MIIC uses. This is a complex set of choices – there are a variety of options, some of which are variations of others. All options do not meet the requirements defined in Section 4, presented earlier; exceptions are noted next. Additional discussion about the relative merits of these options can be found in the Conclusions and Recommendations section presented next. It is important to note that in many cases, the options are not mutually exclusive: multiple strategies can be pursued simultaneously.

Figure 4 depicts the relationship of these options to one another. The table in Appendix A describes each option, its strengths and challenges.

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 interrelated issues. Authentication is a common event and one that consumers encounter every day. For example, 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 users 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/

FOR MORE THAN 20 YEARS, states and other jurisdictions have been collecting data about immunizations for their population in an Immunization Information System, or immunization registry. Granting access to these data for consumers in a public health context can present with both unique opportunities, and challenges.

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 table in Appendix B details options that are available for authenticating and authorizing consumer access to IIS data. Individual organizations 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.

CONCLUSIONS

Minnesota has done no outreach to determine if consumer access to IIS data is desired or demanded. Significant investment in a consumer access strategy for MIIC should be limited until more purposeful engagement with consumers or consumer advocate organizations takes place. There appear to be no other imminent Minnesota consumer health data access initiatives (with the exception of MNsure, the state Health Insurance Exchange). This both reduces any potential points of leverage, as well as potential points of constraint for a consumer access strategy for MIIC.

Other 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 "access/download/transmit" measure may quickly change this. Dominance of Epic as a vendor might provide some particular leverage. State and local public health agencies may provide a point of access for patients without a medical home.

State and MDH technical, legal, and information security staff members are fairly involved in MIIC operations and decision making, so any move toward providing consumer access will require the scrutiny of these offices. This may limit MIIC's ability to move forward quickly or easily. Due to the absence of unique identifiers in MIIC known easily to the outside community (SSN, Medicaid ID, medical record number), consumer access cannot be provided without some level of effort, technical or administrative. 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 MIIC alone without corroborating that relationship with data in MIIC or validating that independently with another source (like the provider).

In terms of the implementation options identified in Appendix A:

- There seems to be less interest in Minnesota in expanding the use of WIR software web client for consumer access (Appendix A, options 1 & 2, variation options 4 & 5), though this is likely the easiest to deploy and access from the consumer's standpoint.
- Creation of a mobile app (Appendix A, option 3) 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 EHR and/or PHR systems (Appendix A, options 6, 7, & 8) require the least modification to MIIC operations and software, but require close cooperation with the EHR/PHR vendors and sites. It is worth noting that authorizing a query user for access to an IIS is significantly easier than authorizing a data submission user. Further investigation of implementations that leverage these options is warranted (see suggested pilot projects next).
- Pursuit of a Blue Button+ strategy is the most forward-thinking of all the options. While the uptake of this new standard is slow nationally, there is significant

UNDERSTANDING LEGAL AND TECHNICAL nuances of granting consumer access to individual health information in public health environments is essential given the emphasis on consumer/patient engagement at both local and national levels.

federal drive behind it. Implementation of this strategy would require the development of some type of publish/subscribe capability (loosely or tightly coupled with the WIR software) and increasing consumer use of Direct messaging to receive the updated notifications and reports.

A pilot project approach would serve Minnesota well. This may involve several pilots, but the main idea is to pilot access to MIIC that requires as little modification to the MIIC software and operations as possible. A project in conjunction with the Southeast Minnesota Beacon Community might allow query to MIIC through normal HL7 query/response and provide access to data to patients associated with that effort, with the burden on the Beacon Community to authenticate and authorize users. A project could also be conducted in conjunction with one or more Epic sites and the MyChart-tethered patient portal that would allow the sites to query MIIC through normal HL7 query/response and provide access to data to patients. The burden would be on the sites to authenticate and authorize users. Finally, a grant-funded implementation of Blue Button+ that would provide a new piece of software to allow a patient to subscribe to a record in MIIC and have an immunization record "pushed" to Microsoft HealthVault via Direct on demand and when an update to the record occurs. This could be done in conjunction with a Minnesota -certified Health Information Organization (HIO) and/or Health Data Intermediary (HDI).

ACKNOWLEDGEMENTS

The authors wish to thank policy analyst Patricia Segal-Freeman, MPH, JD, for her reviews and input to the article, specifically the references to legal language and statutes. Project team would also like to acknowledge the various stakeholders who participated in interviews for their time and expertise. **JHIM**

Noam H. Arzt, PhD, FHIMSS, is president of HLN Consulting, LLC. He has been working with immunization information systems projects for more than twenty years. Arzt can be reached at arzt@hln.com.

Emily Emerson is the assistant director of the Infectious Disease Epidemiology, Prevention and Control Division at the Minnesota Department of Health. She was the manager of the Minnesota immunization information system for nine years prior to this role. Emerson can be reached at emily.emerson@state.mn.us.

Sripriya Rajamani, MBBS, PhD, MPH, is senior health informatician at Minnesota Department of Health. She has been working on informatics and interoperability projects for the department and for the Minnesota e-Health Initiative for past eight years. Rajamani can be reached at sripriya.rajamani@gmail.com.

Katie McGee is a senior business analyst at HLN Consulting, LLC. With over 25 twenty-five years in IT, she has spent the past five years supporting interoperability projects and health information exchange between the clinical community and state HIEs. McGee can be reached at kmcgee@hln.com.

REFERENCES

1. http://www.cdc.gov/vaccines/programs/iis/about.html. *Accessed January, 2014.*

2. http://www.data.gov. *Accessed January, 2014.*

3. http://www.health.state.mn.us/miic. *Accessed January, 2014.*

4. http://www.revisor.mn.gov/statutes/?id=144.3351. *Accessed January, 2014.*

5. http://www.healthit.gov/policy-researchers-implementers/consumer-ehealth-program content.healthaffairs.org/content/32/2/376.abstract. *Accessed January, 2014.*

6. http://www.youtube.com/watch?v=81SBwCENKnA , ONC's Strategy for Engaging Consumers. Presented at the 2012 Consumer Health IT Summit, Washington, DC, September 12, 2012. Accessed January 2014.

7. http://www.va.gov/bluebutton. *Accessed January, 2014.*

8. http://bluebuttondata.org. *Accessed January, 2014.*

9. http://bluebuttonplus.org. *Accessed January, 2014.*

10. http://healthit.hhs.gov/portal/server.pt?open=512&objID=2996&mode=2. *Accessed January, 2014.*

11. www.gpo.gov/fdsys/pkg/FR-2012-09-04/pdf/2012-21050.pdf#12. *Accessed January, 2014.*

12. www.health.state.minnesota.us/clearinghouse/medrecords.html. *Accessed January, 2014.*

13. www.revisor.leg.state.minnesota.us/stats/144/225.html. *Accessed January, 2014.*

APPENDIX A – SOLUTION OPTIONS

Option	Strengths	Challenges
Modify WIR software underlying MIIC to provide a new web-based user interface for consumer access. This new interface accesses the same underlying database as the MIIC provider client. Users can be authorized by MIIC staff, primary care provider with MIIC access, or no one at all (user must substantiate relationship with patient through knowledge of patient demographic details). Users should be able to view a record and download a pdf of the record at minimum.	▪ Allows MIIC to retain control over the user "experience" ▪ MIIC branding is prominent throughout the user's interaction ▪ Common base of data maintained through access to primary MIIC database ▪ 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 ▪ May be possible to leverage software development of other WIR states ▪ Easier to impose two-factor authentication ▪ Potential exposure of PHI in consumers hands limited to immunization data and minimal demographics	▪ Patients will only be able to access information in MIIC database, no more, no less ▪ As usage increases, performance of MIIC database may be negatively affected ▪ May require "negotiation" with state IT over firewall and other security settings and restrictions for consumer access ▪ 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 MIIC using consumer portal instead
Rather than modifying the WIR software itself, create a new, separate, stand-alone web-based interface for consumer access (variation on Option 1).	▪ Allows MIIC to retain control over the user "experience" ▪ MIIC branding is prominent throughout the user's interaction ▪ May be easier for state IT 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 MIIC database may be negatively affected ▪ Limited opportunities to leverage software development of other WIR states unless they embrace this same approach ▪ 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
Create a mobile app to supplement or replace a web-based app for consumer access (variation on Options 1 & 2)	▪ Appeals to current trend in individual computing ▪ Reduces barriers to using application by consumers ▪ Applications tend to be easy to use and intuitive ▪ Easier to impose two-factor authentication	▪ May involve new skill sets for PHA [AU: Expand "PHA". ED: Add to list.] and/or its technical contractors ▪ May provide limited capabilities for printing reports ▪ May require multiple applications for multiple platforms (e.g., iPhone and Android)
Modify MIIC or create a new MIIC module to provide consumer access relying on data from a separate immunization data store (variation on Options 1 & 2)	▪ Allows MIIC to retain control over the user "experience" ▪ MIIC branding is prominent throughout the user's interaction ▪ Potential MIIC database performance impact averted through separate database optimized for consumer query ▪ Enhanced security due to more limited data set in consumer access database ▪ Potential to provide consumer access to other data unrelated to MIIC, including general-purpose health information (i.e., not patient specific but context specific) ▪ May be easier for State IT 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 MIIC database. ▪ Limited opportunities to leverage software development of other WIR states unless they embrace this same approach ▪ 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

Option	Strengths	Challenges
Through a direct web-based user interface, allow patients to download a C-CDA[AU:Expand previous. ED: Add to list.] 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 toward Blue Button+ ▪ Easier to impose two-factor authentication	▪ Clinical documents (C-CDA) represent new territory for most public health agencies; limited training and experience
Allow EHR systems to query MIIC for patient records and forecast via HL7 v2 messages. Encourage patient access through interfaces provided by provider organizations.	▪ No modifications to MIIC 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 MIIC 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 7 simultaneously	▪ MIIC loses much control over the user's "experience" including what data are provided and in what format ▪ Dependent on providers' implementation of MIIC HL7 query and proper processing of responses. ▪ As query usage increases, performance of MIIC may be negatively affected ▪ Current "read-only" CCOW [AU: Expand previous. ED: Add to list.]-enabled EHR query of MIIC 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
Allow authorized PHR systems or HIE to query MIIC for patient records and forecast via HL7 v2 messages. Patient access is the provided through PHR account. MIIC 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 ▪ PHRs more likely to display longitudinal (versus encounter-based) data	▪ 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
Allow EHR and/or PHR systems and/or HIE to query MIIC for patient records and forecast via HL7 v2 messages, but return a C-CDA document	▪ Consistent with Options 5 and 6 ▪ More consistent with emerging format for electronic medical records interoperability ▪ Can be implemented independent of current MIIC software through web services (i.e., new web service intercepts EHR/PHR query, sends query on to MIIC, receives data and converts to C-CDA)	▪ Same as Options 5 and 6 ▪ Clinical documents (C-CDA) represent new territory for most public health agencies; limited training and experience ▪ Harder to impose two-factor authentication
Implement Blue Button+, which allows patients to "subscribe" to records in MIIC 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

APPENDIX B – ACCESS CONTROL OPTIONS

Option	Strengths	Challenges
No specific authentication other than knowledge of enough data to successfully query and return a single result. Data might include: First name Last name Date of birth 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
No specific authentication other than knowledge of enough data to successfully query and return a single result (similar to previous option 1) including at least one unique identifier which might be: Social Security Number Medical Record Number MIIC ID Medicaid ID (e.g., WIR, NESIIIS)	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
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
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 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 MDH or 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 that of Option 3