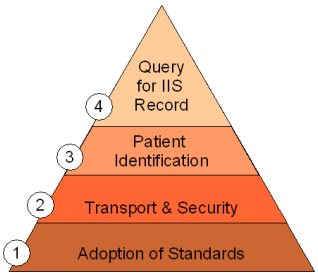
Focus Area #2: Transport & Security

Background Material

This focus area concerns various areas ranging from standards used to send messages to methods used to ensure that the query is being conducted by an authorized clinician for an authorized use.



Information for the Group

In order for the group to understand this section they will need to be familiar with:

- HTTPS
- Transport Layer Expert Panel (TLEP) WSDL
- HL7 v2 queries (QBP)

This information for the group is not covered here in the background material.

Included Information

Review the document *Architectures and Transport Mechanisms for Health Information Interchange of Clinical EHR Data for Syndromic Surveillance*.

Transport Standard

A common transport standard is critical for Meaningful Use 3 as HL7 messages will need to be submitted and processed in real-time. This requires that the IIS community promote and support a common transport standard.

Two years ago the immunization community selected SOAP/Web Services as the preferred method for transmitting HL7 messages. A standard definition of this web service, called a WSDL was developed and disseminated by CDC's IISB. This method is now be adopted by various IIS. Despite this the following issues remain:

- So far, only a handful of IIS have implemented this method.
- This method is specific to IIS and is not shared by any other standard.

Decision Point

	Recommend	Permit	Discourage
IIS should make available a TLEP compatible interface.			
EHRs should be able to support TLEP standard.			
IIS community should consider adopting a different transport standard.			

Direct Connection to IIS

Creating a connection from every EHR in a state to the IIS can be a very daunting task for many reasons:

- IT department policies at the state level are often very restrictive, risk adverse, and usually a barrier to public health policies.
- IT department policies are increasingly requiring complicated two factor authentication schemes.
- Connecting individual organizations to the IIS can take a great deal of IIS staff time.
- Outside organizations, particularly smaller organizations have neither the time nor technical capability to meet IT department policies.

One solution to this problem is to move the task of connecting to local providers to an intermediary party. This can include the following solutions:

- Health Information Exchange
- EHR vendor's centralized messaging system
- Other clearinghouse

A clearinghouse is an outside system that receives data and then moves it on to its final destination. This is a common model in other areas, such as submitting patient claims. The clearinghouse allows for easy connections to the local site, without the red-tape and requirements of a State IT department, while the clearinghouse does basic checks and relays this information to the IIS. In its most basic form, an HEI is a clearinghouse.

Assignment
Discuss the movement away from direct connections. Will this be the norm in the future? What should IIS be ready for? What are the decision points we need to make?

Identify Risks

IIS face risks when opening their interface to respond to queries. Some of these risks include:

- Unauthorized persons querying for records.
- Authorized persons querying for records for the wrong purpose.

Assignment
Identify all the security risks that IIS face specifically for queries.

Authentication

The TLEP standard has built-in support for single factor authentication. Two factor authentication is possible, and can be implemented on top of the TLEP standard, and doing so is left to the decision of the IIS. Because of this there are different standards being used for authentication, some at the message level and some at the certificate level.

Two Factor Authentication
Two factor authentication is a process of using two different kinds of information to authenticate a person. For example, to withdraw money from an ATM a person must both have the correct ATM card

and know the secret PIN. A person may pick-pocket the ATM card, or someone else might guess the 4 digit PIN, but to do both is quite difficult.

Access to the IIS is often controlled by IT department policy, which as the following issues:

- IT departments are often not concerned with the goals and needs of the IIS program. They are not responsible with the success of the IIS.
- IT departments are focused on the risks. If there is a security problem they are responsible.
- It is the best interest of the IT department to support transport methods they are familiar with and represent to them the least security risk.
- IT department policies continue to change and are moving towards reducing risks and limiting connections.

All of this points towards the adoption of two factor authentication schemes. This process has a negative impact on providers wishing to connect to the state. Many of these immunization providers have the following characteristics:

- Very little technical support and expertise. While the IIS may have an IT department the pediatric physician may be the only one available to help connect to the IIS.
- Low usage of connection. Many smaller providers may not be able to justify the cost of time to integrate with an IIS when so little information will actually be transferred. The layer of security and red-tape cancels the benefit.
- Very limited software and hardware availability and no budget for additional hardware or software to support interchange.
- A very low tolerance for dealing with technical issues. Most small practices need easy solutions or they will not want to bother. They are in the practice of giving patient care, not in jumping through technical hoops that make no sense to them just to meet the requirements of a government IT department.

It is important to discuss that there needs to be a solution that provides the correct level of security while not stifling the ability of the IIS to become the center of patient's immunization record.

Another important point about setting standards, and this applies to all the points in this meeting, but most particularly to this one. An adoption of a national standard that meets 80% of the use cases out there does NOT preclude an IIS from allowing other entities to connect in other ways with other levels of security. A national standard is not a requirement that all interfaces be done a certain way but rather that a standard way is available at all IIS. Just like requiring all businesses to have a valid postal address so they can receive US Mail does not prevent any business from receiving packages from FedEx. The discussion should not focus on the current operating interfaces, these do not have to change even if a newer standard is adopted.

Decision Point

	Recommend	Permit	Discourage
TLEP standard is well enough defined, no more			

development needed.			
IIS community should standardize a method or two methods (or perhaps even three) for two factor authentication.			
IIS community should further standardize the use of MSH and other HL7 message fields for the purpose of authenticating and identifying the sender.			

Sender Identification

Currently every IIS has a different method for identifying the sender of a message. Various IIS have identified senders by:

- Using security tokens in the message transport (username/password).
- Using the MSH-4 headers to request the EHR to set a specific value.
- Using BHS-4 field to request the EHR to set a specific value.
- Using other headers in the MSH segment.
- Requesting EHR to use OIDs in MSH segments.
- Using other fields in the HL7 message.

Decision Point

	Recommend	Permit	Discourage
IIS community should decide on one or two standards for identifying the sending system.			
Leave current IIS variability as is.			

Sender Identification for Aggregated Data Feeds

One of the areas for special discussion is how should the sender be identified for data feeds from EHR vendors who centrally host many different providers. Should the EHR vendor send each provider as a different feed, or can all of them be sent in the same feed?

Assignment

Discuss sender identification within the context EHR vendors who aggregate data from many different otherwise unconnected providers. Create the appropriate decision points.

Organization Mismatch

The IIS organizes submitting systems into various collections of organizations and facilities. These organizations often reflect the IIS project needs and may not line up with how EHR systems are deployed or how submitting organizations are structured. The following problems can happen:

- The EHR is used by a single completely integrated organization that is seen as two separate distinct organizations by the IIS.
- The EHR is used by an integrated organization with different sub organizations that is seen by the IIS as a single organization.
- The EHR may be used by an integrated organization where the organizational structure and divisions differ from the IIS's view of the organization.

- The EHR is deployed separately at different locations, all of which are considered a single integrated organization by the IIS.

These organizations mismatch means that EHR's are often requested to:

- Put all data from disparate data into one coherent feed.
- Report data from a single system using two different accounts. The EHR must take extra steps to determine which data should be submitted under which account.
- Report data that is identified under a organizational identification system that does not match the IIS.

While this mostly involves the reporting of data, this impacts queries because the IIS needs to know the context for how the patient id is stored and how to find patients when the EHR queries again. It may be very difficult for EHR vendors to determine how to query the IIS when the patient may have been reported under two different submission accounts.

Assignment
Discuss problem and determine if there is any way that this could be standardized nationally?

Query Tracking

Authentication normally authenticates the sending system but not the user who actually initiates the query. This is because managing external users is very complex. For the purposes of auditing queries it is critical for both IIS and EHR to track:

- EHR username of the person initiating the query.
- The reason why or the purpose for which the user is initiating the query.

The EHR username would not be entered by the user, but would rather be known by the EHR when the query was made as the user should be authenticated to the EHR before being able to query. This would be an easy field for the EHR to generate.

The text for the reason or purpose would also be generated by the EHR and would indicate in a human readable way what activity the user was conducting that gives context for the query request. This requirement was suggested as something that may be asked for by future HIPAA regulations. Since the information would be easy for an EHR to generate, it would be good to add to the standard now.

For both of these fields the IIS could use them or ignore them.

Decision Point

	Recommend	Permit	Discourage
Create requirement for query messages to include the EHR username and text giving the reason the user is initiating the query.			
IIS should log, for auditing purposes, the EHR username, text reason for query, time of query, and			

patient returned.			
EHR should log, for auditing purposes, the EHR username, text reason for query, time of query, and patient returned.			

Artifacts Needed

For the purposes of discussion the group needs to create the following items:

- Use case story(ies)
- Use case diagram(s)
- Lessons learned
- Decision points
- Recommendations
- Known needs
- Next steps

Use Case Story

A use case story is a list of steps taken by a user and the interaction of systems to achieve a specific goal. The goal of this focus area is to select a single use case but other use cases stories should be written as well if they are to be discussed in detail.

Use Case Diagram

Diagrams give a visual map to the story. Every use case story must have a corresponding diagram.

Lessons Learned

Past experience helps when making future plans. Gather information about lessons learned when implementing query support. Be sure to include lessons learned from both the IIS and the EHR perspective.

Decision Points

What are areas that need to be decided by the group? What are the options? What are the benefits and risks with each option?

Recommendation

What is the recommendation of the group for each decision point? If the group is divided then list the two or three top recommendations.

Known Needs

For each recommendation, list what support or help the EHR and IIS will need in order to meet the recommendation.

Next Steps

For each recommendation, list the next steps that will need to be taken.