

Working Together on Data Exchange: a Guide to Indian Health Service (IHS) and State Immunization Information System (SIIS) Interfaces

Developed by the
IHS Immunization Program,
IHS Division of Epidemiology and Disease Prevention
Albuquerque, NM





DEPARTMENT OF HEALTH & HUMAN SERVICES

Indian Health Service
Division of Epidemiology and
Disease Prevention
5300 Homestead Road, Northeast
Albuquerque, NM 87110
(505) 248-4132

January 16, 2008

TO: Indian Health Service Area Directors
Indian Health Service Chief Medical Officers

FROM: Director, Indian Health Service Division of Epidemiology and Disease Prevention
Director, Indian Health Service Office of Public Health Support
Acting Chief Medical Officer, Indian Health Service

SUBJECT: Release of Data Exchange Guide from the Indian Health Service
Immunization Program

As an HHS agency, the IHS is committed to the Healthy People 2010 objective to "increase to 95% the proportion of children aged <6 years who participate in fully operational, population-based immunization registries" (Objective 14-26). To this end, the HHS Centers for Disease Control and Prevention funds state immunization programs to develop and maintain state immunization information systems (SIIS). Recognizing the value of SIIS, the 2006-2011 IHS Strategic Plan seeks to achieve interoperability between disparate systems, and supports developing ongoing data sharing relationships with Tribal Epidemiology Centers, state, federal and private entities, including facilitating immunization data interfaces with SIIS. (Objective 2.6)

The Division of Epidemiology and Disease Prevention is pleased to announce the release of the IHS Immunization Program's, "*Working Together on Data Exchange: a Guide to Indian Health Service (IHS) and State Immunization Information System (SIIS) Interfaces*". The guide introduces the IHS data exchange initiative, informs participants of the interface requirements and provides the groundwork for further discussions between IHS and SIIS. We hope that this guide will lead to enhanced immunization data for RPMS users throughout the IHS, tribal and urban (I/T/U) Indian healthcare system and feel it reflects our Division's continued commitment to working in the spirit of partnership with other agencies on behalf of IHS clinical populations.

Please distribute to immunization providers and IT staff. For more information, please contact Cecile Town, IHS Immunization Registry Coordinator, 505-248-4233 or cecile.town@ihs.gov.

James E. Cheek, MD, MPH, Director
Division of Epidemiology and Disease Prevention

Richard M. Church, Pharm.D, Director
Office of Public Health Support

Charles North, MD, MS, Acting Chief Medical Officer
Indian Health Service

Enclosure

Dear Colleague:

The Indian Health Service (IHS) National Immunization Program is a partnership between the Centers for Disease Control and Prevention (CDC) and IHS, working with IHS, tribal and urban Indian (I/T/U) immunization programs across the country. The program is based in the IHS Division of Epidemiology and Disease Prevention in Albuquerque, NM and the staff are field assignees from the CDC Immunization Services Division.

As HHS agencies, CDC and the IHS are committed to the Healthy People 2010 objective to “increase to 95% the proportion of children aged <6 years who participate in fully operational, population-based immunization registries” (Objective 14-26). To this end, CDC funds states and provides technical assistance to develop and maintain state immunization information systems (SIIS), or registries. Recognizing the value of SIIS, the 2006-2011 IHS Strategic Plan seeks to achieve interoperability between disparate systems, and supports developing and supporting ongoing data sharing relationships with tribal, state, federal and private entities, including facilitating the exchange of immunization data with SIIS.

What follows is a guide to the IHS initiative to establish immunization data interfaces between SIIS and the IHS Resource and Patient Management System (RPMS) used by many I/T/U healthcare facilities nationwide. It is designed to introduce the initiative, familiarize personnel with the software and participation requirements, and create a foundation for further discussions between SIIS personnel and the IHS Immunization Program.

IHS recognizes that SIIS are a critical tool for increasing and sustaining vaccination coverage and we look forward to working together towards RPMS/SIIS interfaces.

Sincerely,

Cecile Town, MPH
CDC Research Officer
IHS Immunization Registry Coordinator

Amy Groom, MPH
CDC Public Health Advisor
IHS Immunization Program Manager

Table of Contents

Background	1
Software Needed.....	2
Immunization Data Interface: The Process.....	3
Participation Requirements for establishing an interface between the IHS RPMS and SIIS	4
Getting Started with Data Exchange.....	5
Sample Test Message, HL7 Format.....	6
Variables that IHS sends to the SIIS.....	7
Data Sharing Agreements with I/T/U Partners.....	9
IHS Data Exchange FAQ's.....	10
Appendix A: The IHS Data Sharing Policy Memo.....	12
Appendix B: Transport of Immunization HL7 Transactions Over the Internet Using Secure HTTP, Ver. 1.0	16

The Indian Health Service (IHS) Immunization Data Interface

Background

Medical record scattering is a common problem and can affect patient care. For immunizations, incomplete information can lead to over or under immunization and wasted resources. CDC has supported the development of state immunization information systems (SIIS) to address these issues.

The Indian Health Service (IHS) supports an electronic medical record, called the Resource and Patient Management System (RPMS), which is used by many IHS Tribal and Urban Indian (I/T/U) programs. The RPMS contains an immunization module for entering and tracking immunizations, and data are stored at the local facility. RPMS data are usually not included in SIIS as it may not be feasible for sites to enter the immunizations they provide into 2 systems (the RPMS and the SIIS).

The IHS Immunization Data Exchange initiative has resulted in the development of software to enable an automated, two-way batch RPMS/SIIS interface. The IHS immunization data exchange software, called BYIM, extracts immunization data from the RPMS system and sends a batch file to the SIIS using standard Health Level Seven (HL7) messages in accordance with CDC's national immunization registry data exchange standards. In response to the data sent from the RPMS, the SIIS creates a file of immunizations missing in the RPMS data to be retrieved by the I/T/U facility. This information can then be downloaded into the RPMS, alleviating the need for staff to enter the information into the RPMS, and ensuring that a patient's complete immunization history is available to the provider.

This software was released nationally in March 2006 and an updated version will be available in 2007. This initiative will improve patient care by providing more complete immunization data on children served by I/T/U sites to all providers, thereby ensuring appropriate immunization.

What follows is a guide developed by the IHS Immunization Program for states and I/T/U sites who are interested in using HL7 messaging to do bi-directional immunization data interfaces.

Software Needed – all installed at IHS sites

1 – Immunization module of the IHS Resource and Patient Management System (RPMS)

- An RPMS module designed to record, store and manage patient immunization information
- Information entered into the package is integrated into other health information in RPMS such as laboratory, pharmacy, etc.
- Functions include:
 - Tracking and forecasting of immunizations
 - Immunization coverage reports
 - Reminder/ recall letters
 - Due lists
 - Doses Administered Report
 - Vaccine Inventory

2- IHS Immunization Data Exchange (BYIM) software

- Bi-directional
- HL7 Message (2.4)
- Batch files extracted from IHS RPMS
- Conforms to CDC's *Standard Protocol for Immunization Data Transactions Using HL7*
- Uses HTTPS to transfer files
- Relies on state de-duplication process
- State sends reciprocal file with any new immunizations
- Data “reviewed” and imported into RPMS

Note: The SIIS cannot connect independently to the IHS RPMS servers. The IHS site must initiate an HTTPS connection to the SIIS before receipt of the return message can take place.

3 – HL7 Communications Bridge software

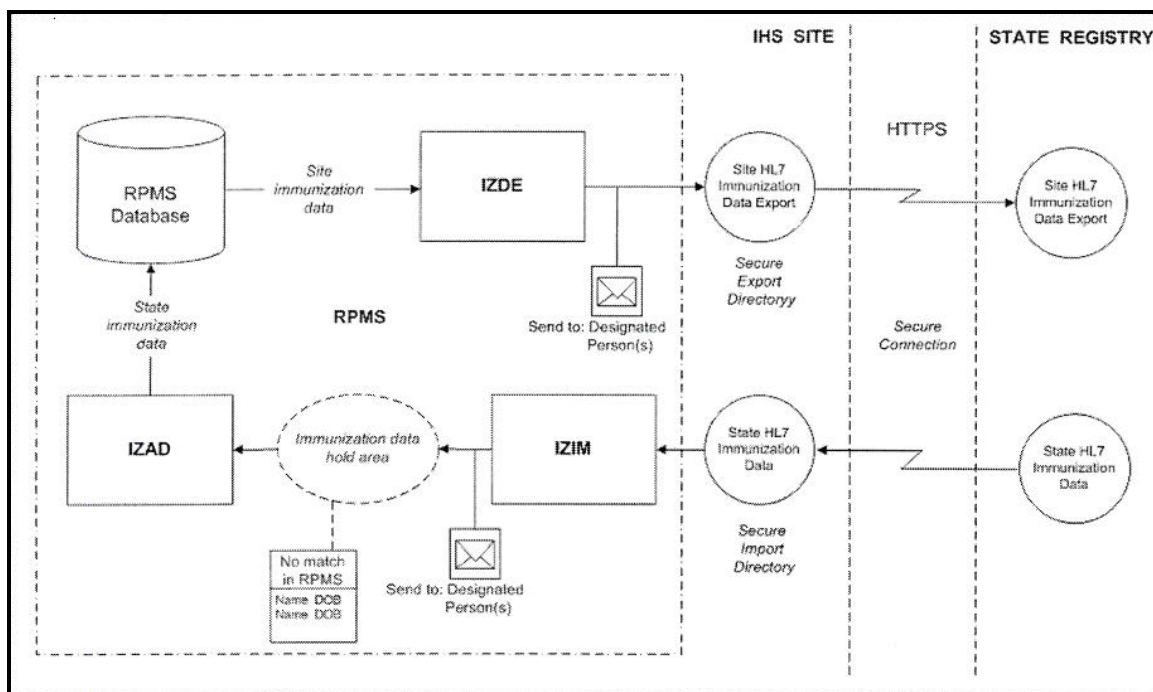
- An IHS-licensed STC software product that automates the interface on the IHS side
- License covers any IHS, tribal or urban site that uses RPMS
- Operates in conjunction with BYIM 1.01
- Enabled via a secure HTTPS connection that connects with the state registry. The SIIS must provide the secure HTTPS connection.
- Downloaded at the IHS site
- No cost to the state to support

These software products are provided to sites by the IHS, and are designed to be used in conjunction with one another to exchange immunization data with the SIIS. SIIS programmers and developers will need to be involved early on to determine the interoperability of the IHS software with the SIIS. The IHS Immunization Registry Coordinator can facilitate communication between SIIS and IHS personnel as needed.

Immunization Data Interface: The Process

The IHS Immunization Data Exchange Software, referred to as BYIM, is installed at participating I/T/U sites. Each site will also install the HL7 Communications Bridge software, which works with the BYIM to bi-directionally automate the interface in states with a secure web portal.

1. With the IHS BYIM, the user exports a file consisting of the entire immunization record for all patients < 19 years with a visit since the last export to a secure export directory (IZDE command). The frequency of exports is determined by each facility. Daily exports are recommended.
2. The HL7 Communications Bridge detects a file in the export directory and connects it to the state registry through a secure internet HTTPS connection, which then transmits the file as an HL7 batch file.
3. The state registry or SIIS receives the file via HTTPS and parses the data.
4. At the same time and on the same secure HTTPS connection, the HL7 Bridge will pick up an import file (if one is present) from the SIIS and place the file into the import folder in a secure local directory. This file includes any vaccines sent to the SIIS by other providers since the site's last SIIS import.
5. Using the BYIM IZIM command, the SIIS reciprocal file is imported into RPMS. The data are extracted and BYIM matches the patients in the SIIS file with patients in the RPMS, places the data in a holding area, and sends an email notification that the immunization data have been imported into RPMS. Any non-matching patients are written to a list.
6. An I/T/U clinical person with immunization expertise reviews the individual patient vaccine data and adds it into the individual patient's electronic RPMS record (IZAD command). This process can be automated at the I/T/U clinic level.



Participation Requirements for establishing an interface between the IHS RPMS and SIIS

I/T/U sites should:

1. Use the IHS Resource and Patient Management System (RPMS)
2. Designate an IT contact who can work to download, install and set-up the BYIM and Bridge software, as well as enable the site's SIIS account.
3. Designate a clinical contact who will conduct exchange activities. Such as: generating the RPMS export and reviewing and adding data received back from the state into RPMS. This person will need to familiarize themselves with the BYIM software.
4. Download and install BYIM v 1.01
5. Download and install the HL7 Communications Bridge software
6. Set up a registry account with the SIIS
7. Coordinate with the SIIS for test messaging
8. Run reports before and after initial data exchange for submission to the IHS Immunization Program
9. Communicate with the IHS Immunization Registry Coordinator for technical assistance

SIIS should:

1. Have the capability to send & receive HL7 batch messages
2. Have a secure web site/portal to support the Bridge connection
3. Complete an IHS Interconnection Security Agreement (ISA) and update it annually. Where applicable, the IHS Immunization Registry Coordinator will provide this document.
4. Have the ability to track the patients sent to the SIIS by keeping a log of all the patients each site sends to the registry
5. Have the ability to send a reciprocal file back to each site that includes data from other providers the patient visited. This will be new data that was not contained in the export from the site.
6. For the reciprocal file, the SIIS should send back the same patient demographic data provided in the RPMS export file, not the demographic data contained in the SIIS. This will aid the IHS matching algorithm in BYIM.
7. As with other participants, provide I/T/U sites access to the SIIS.
8. Communicate with IHS Immunization Program staff, I/T/U site IT staff, programmers and developers to facilitate the testing process.
9. Provide technical support to I/T/U site users in the set-up, testing and use of the registry.

The IHS Immunization Program will coordinate communication with regard to data exchange and facilitate technical assistance.

Getting Started with Data Exchange

People work together on many levels to establish, build, test and maintain the data exchange process. From our experience, the SIIS, the IHS National level Data Exchange Team (DET) and the IHS, Tribal or Urban (I/T/U) site teams all have programmatic as well as technical personnel who work together at various stages towards a successful interface.

Stage 1 – Initial Q & A

This involves the initial communication indicating interest and determining interoperability (see pg. 4). SIIS personnel will communicate with the IHS DET, via the Immunization Registry Coordinator. At this time, the IHS DET will also work with the SIIS to complete the IHS Interconnection Security Agreement (ISA) in states where this is applicable (see pg. 9)

Stage 2 – Getting Started - SIIS

States will engage their SIIS personnel in conference calls with the IHS DET (Immunization Registry Coordinator, Developers, Programmers, Contractors) so that the technical staff are able to determine system specifications that will enable data exchange. A timeline for testing is established.

Stage 2 – Getting Started – I/T/U

I/T/U sites that would like to establish an interface with the SIIS begin to work with the IHS DET to get set up by establishing IT & clinical contacts for the exchange process and installing the BYIM and Bridge software. After the software is installed, the I/T/U site must also work with the SIIS personnel to establish a site account with the SIIS and a secure HTTPS connection for the Bridge.

Stage 3 – Test Messaging

The IHS DET will work with the I/T/U site to send a sample test message to the SIIS. SIIS personnel may also be involved. When this is done successfully, the IHS DET contacts the SIIS personnel to begin the testing phase using real RPMS immunization data. At this time, the IHS DET trains the I/T/U site contacts on running BYIM for the interface.

Stage 4 – Testing Phase

The I/T/U site contact will examine data received back from the SIIS prior to adding it back to RPMS. If issues arise, the I/T/U site will work with the IHS DET or the SIIS personnel as necessary.

Stage 5 - Production

Once the process can occur without “bumps”, the site is ready to automate the exchange by engaging the HL7 Communications Bridge Software, which should already be installed.

Sample Test Message, HL7 Format

IHS sends to the IIS

```
FHS|^~\&|IZ REGISTER|CHINLE HOSP|||20070807043010-0700
BHS|^~\&|IZ REGISTER|CHINLE HOSP|||20070807043010-0700
MSH|^~\&|IMMUNIZATION REGISTER|CHINLE HOSP|||20061219043046-0700|VXU^V04|IHS-3914454|P|2.4|||AL|AL|
PID|1|111694|808101111694^^^^MR|DEMO^PATIENT^MIDDLE^^^|DEMO^MOTHER^MIDDLE^^^|20061104|F||1002-5|BOX
XYZ^^CHINLE^AZ^86503|||999887777|
NK1|1|DEMO^MOTHER^MIDDLE^^^|MTH^MOTHER^HL70063|BOX XYZ^^CHINLE^AZ^86503|928 594 9999 C||NOK^NEXT OF
KIN^99IHS|
RXA|0|1|20061218133600|19890620120000|110^DTaP-Hep B-IPV^CVX|.5|||00^NEW IMMUNIZATION RECORD^NIP001||CHINLE
HOSP^^^CHINLE HOSP|||AC21B074AA|SKB^GLAXOSMITHKLINE^MVX|
RXA|0|1|20061218133600|19890620120000|49^HIB (PRP-OMP)^CVX|.5|||00^NEW IMMUNIZATION RECORD^NIP001||CHINLE
HOSP^^^CHINLE HOSP|||0403F|MSD^MERCK & CO.^MVX|
RXA|0|1|20061218133600|19890620120000|100^PNEUMOCOCCAL CONJUGATE^CVX|.5|||00^NEW IMMUNIZATION
RECORD^NIP001||CHINLE HOSP^^^CHINLE HOSP|||B08675H|WAL^WYETH-AYERST^MVX|
RXA|0|1|20061218133600|19890620120000|116^ROTAVIRUS, PENTAVALENT^CVX|2|||00^NEW IMMUNIZATION
RECORD^NIP001||CHINLE HOSP^^^CHINLE HOSP|||0776F|MSD^MERCK & CO.^MVX|
MSH|^~\&|IMMUNIZATION REGISTER|CHINLE HOSP|||20061219043046-0700|VXU^V04|IHS-3914453|P|2.4|||AL|AL|
PID|1|111694|808101111694^^^^MR|DEMO^PATIENT2^MIDDLE^^^|DEMO^MOTHER2^MIDDLE^^^|20051204|F||1002-5|BOX
XYZ^^CHINLE^AZ^86503|||999887777|
NK1|1|DEMO^MOTHER2^MIDDLE^^^|MTH^MOTHER^HL70063|BOX XYZ^^CHINLE^AZ^86503|928 594 9999 C||NOK^NEXT OF
KIN^99IHS|
RXA|0|1|20060324120000|19890620120000|110^DTaP-Hep B-IPV^CVX|999|||01^HISTORICAL INFORMATION - SOURCE
UNSPECIF^NIP001||OTHER^^^OTHER|||^^MVX|
RXA|0|1|20060526120000|19890620120000|110^DTaP-Hep B-IPV^CVX|999|||01^HISTORICAL INFORMATION - SOURCE
UNSPECIF^NIP001||OTHER^^^OTHER|||^^MVX|
RXA|0|1|20060726120000|19890620120000|110^DTaP-Hep B-IPV^CVX|999|||01^HISTORICAL INFORMATION - SOURCE
UNSPECIF^NIP001||OTHER^^^OTHER|||^^MVX|
BTS|399
FTS|1
```

Where:

FHS = File Header Segment	NK1 = Next of Kin/Associated Parties Segment
BHS = Batch Header Segment	RXA = Pharmacy Administration Segment
MSH = Message Header Segment	BTS = Batch Trailer Segment
PID = Patient Identification Segment	FTS = File Trailer Segment

Variables that IHS sends to the SIIS:

FHS File Header Segment

1. File Field separator = |
2. File Encoding Characters
3. File Sending Application
4. File Sending Facility
5. Not used File Receiving Application
6. Not used File Receiving Facility
7. File Creation Date/Time
8. Not used File Security
9. Not used File Name/ID/Type
10. Not used File comment
11. Not used File Control ID
12. Not used Reference File Control ID

MSH Message Header Segment

1. Field separator
2. Encoding Characters
3. Sending Application
4. Sending Facility
5. Receiving Application
6. Receiving Facility
7. Date/Time of Message
8. Not used Security Type
9. Message type
10. Message Control ID 3
11. Processing ID
12. Version ID
- 13 – 14 Not used
15. Accept Acknowledgement type = AL
16. Application Acknowledgement type = AL

PID Patient Identification Segment

1. Set ID – PID
2. Patient ID = local/RPMS 6 digit Med Record #
3. Patient Identifier list
4. Alternate patient ID – PID
5. Lastname^firstname^middle (patient name)
6. Lastname^firstname (mother's maiden name)
7. Date of birth
8. Sex (M or F or Unknown)
9. Not used Patient Alias
10. Race = 1002-5 = AI/AN
11. Mailing Address
- 12 – 18 Not used
19. SSN Patient

NK Next of Kin/Associated Parties Segment

1. Set ID NK1
2. Lastname^Firstname
3. Relationship = example MTH^MOTHER^70063
4. Mailing address
5. Phone Number
6. Not used = Business Phone Number
7. Contact Role NOK^NEXT OF KIN^99IHS
- 8 – 32. Contact data elements – Not Used

RXA Pharmacy Administration Segment

1. 0
2. Not used
3. Date of Vaccine
4. Date of data transfer
5. Vaccine CVX code^Vaccine name^CVX = 03^MMR^CVX
- 6 – 8 Not Used
9. 01 = Historical 00 = Administered
10. Not used
11. Facility
- 12 -14 Not used
15. Lot #
16. Not used
17. Manufacturer --- see MVX if Lot # was documented

Data sharing agreements with I/T/U partners

The IHS recognizes that under HIPAA, sharing immunization data with state registries is permitted and the IHS Strategic Plan 2006 – 2011 specifically supports data sharing relationships with entities such as immunization registries. To that end, the agency issued a policy memo (Appendix A) which states that sharing data with state registries is permitted and encouraged.

However, there is no requirement for I/T/U facilities to share data with states. From the policy memo:

“disclosures made pursuant to a routine use are discretionary, not mandatory”

This statement takes into account the sovereignty of each tribal nation and their individual government to government relationships with the United States. Related to data exchange, it means that ultimately, participation is determined by the tribe.

Separate from any Memorandums of Understanding (MOU) that a SIIS may require from registry participants, the IHS will require an Interconnection Security Agreement (ISA) from state registries who will establish immunization data interfaces with IHS facilities in their state. While a MOU will cover organizational responsibilities and scope of work, an ISA will identify and implement information security safeguards and responsibilities required for the establishment of the interface.

With consideration to the IHS infrastructure in various states, it may not be a requirement for each state to complete an ISA. Please contact Cecile Town, IHS Immunization Registry Coordinator, at (505) 248-4233, for more information about the ISA.

IHS Data Exchange FAQs

1. What is the IHS Immunization Data Exchange System?

The IHS Immunization Data Exchange System (BYIM) is software developed by IHS to create CDC compliant HL7 messaging to facilitate bi-directional immunization interfaces with SIIS. The software is loaded at the I/T/U site and extracts immunization data from the RPMS and converts it into an HL7 message file. This file can then be sent to the SIIS. The SIIS in turn generates a file with immunization data for those patients that were missing in the RPMS file, and sends it to the site for importation into RPMS.

2. In what states is this working?

Beta – testing of BYIM was completed at pilot sites in AZ, MN, WA and WI. This software is available for use by all I/T/U sites that use RPMS. In AZ and WA data exchange has expanded beyond the initial pilot sites. As of January 2007, 16 sites in AZ and 8 sites in WA were exchanging data with the SIIS using the BYIM and Bridge software.

3. What is the format of the HL7 messages generated by BYIM?

BYIM generates HL7 messages following the standards laid out by the CDC in the Implementation Guide for HL7 messages

<http://www.cdc.gov/vaccines/programs/iis/stds/downloads/hl7guide.pdf>

4. What version of HL7 is used?

BYIM uses HL7 Version 2.4

5. What patients are included in each file? Do the files just contain new immunizations since the last export, or all immunizations?

The initial file sent from RPMS to the SIIS will include all patients < 19 years, and will include the complete immunization history for each patient. For subsequent exports, BYIM sends the complete immunization history for any patient < 19 years who has had a clinic visit since the last export, regardless of whether or not they received an immunization at the visit.

6. How are the files transmitted?

There are two ways the data are sent from the RPMS to the state: a “manual” process, and an “automated” process. The manual process requires someone to log on to the state site and transfer the data file each time it is generated. They must also log on to collect the state’s return file before integrating it back into RPMS.

The automated process uses an HL7 Communications Bridge to establish an HTTPS connection to a state’s secure web portal. Through this connection, data can be sent to the state and also retrieved from the state and transferred back to the RPMS (see Immunization Data Interface: The Process p. 3).

7. Will IHS be sending batch files or will data be exchanged in real time?

The BYIM software currently sends batch files. Frequency of batch file transmission can be determined by the site.

8. Does the BYIM software need to be loaded on the SIIS for this to work?

No. The BYIM software is loaded only on the RPMS side. However, states may need to make modifications or enhancements to their SIIS in order for their SIIS to correctly interpret the HL7 2.4 vaccine data message and load the vaccine data into their SIIS.

9. Will we need funds to get this up and running in my state?

It depends. IHS has a contract for general technical support to roll out to I/T/U sites using RPMS, so costs on the I/T/U end are covered. However, if a state needs to modify their SIIS for this interface, the state will need to support those costs.

10. Will the RPMS data we receive from I/T/U sites be de-duplicated?

No. There is no state-level repository of information for I/T/U RPMS data. Each site will send their information directly to the SIIS. The SIIS will need to de-duplicate data.

11. How can I get this going in my state?

The first step is to review “Working Together on Data Exchange: a Guide to IHS and SIIS Interfaces”, to ensure your registry has the ability to receive and send the CDC approved HL7 messages using a HTTPS secure connection. Initially, we recommend that the interface is piloted at one I/T/U site in the state. It is important to identify a site that has good IT support and a supportive clinical person who can review and understand immunization data to ensure the process is working correctly.

12. Can tribal or urban Indian health programs also participate in the interface?

Yes. The BYIM and HL7 Communications Bridge software can be used by any healthcare site in the I/T/U Indian healthcare system that uses RPMS. I/T/U sites who do not use RPMS should contact the SIIS for more information about participation.

13. Who can I contact for more information?

IHS has an immunization registry coordinator who serves as the central point of contact for all exchange inquiries:

Cecile Town, MPH - IHS Immunization Registry Coordinator
e-mail: Cecile.Town@ihs.gov
Phone: (505) 248 – 4233

She can refer state and IHS partners, as needed, to the other members of the IHS Data Exchange team: Amy Groom, MPH - IHS Immunization Program, Albuquerque, NM; Scott Hamstra, MD – Sells Indian Hospital, Tucson, AZ; John Parker, RN - Chinle Comprehensive Health Care Facility, Chinle, AZ

Appendix A: The IHS Data Sharing Policy Memo



AUG 14 2001

TO: See Below

FROM: Privacy Act Officer, IHS

SUBJECT: Clarification of September 11, 2000 Policy Statement for Sharing Indian Health Service Data with State Health Department Immunization and Other Registries

This memorandum supercedes the September 11, 2000 memorandum issued by the IHS Chief Medical Officer, subject: Policy statement for sharing IHS data with State Health Department Immunization and Other Registries. This action is prompted by the numerous concerns and questions raised by IHS Area and Service Unit staff and IHS Office of General Counsel (OGC) Regional Attorney staff concerning the guidance and their requests for clarification of the guidance.

The following provides guidance regarding the sharing of IHS patient data with State and other registries, e.g., a State health department immunization, cancer, STD, birth defect, or other health care registry and is effective immediately.

In a July 21, 1998 memorandum to the IHS Privacy Act Officer, the Office of the General Council (OGC) provided general guidance concerning data-sharing with State or other registries. OGC suggested that IHS may disclose its health data with State and other registries in accordance with routine use nos. 1 or 7 contained in Privacy Act System of Records-Health and Medical Records Systems, 09-17-0001. 58 FR 36208 (July 6, 1993). However, IHS must first ascertain that the registry fulfills routine use nos. 1 or 7 criteria discussed below.

Routine Use I: *"Records may be disclosed to State, local or other authorized organizations which provide health services to American Indians and Alaska Natives or provide third-party reimbursement or fiscal intermediary functions, for the purpose of planning for or providing such services, billing or collecting third-party reimbursements and reporting results of*

medical examination and treatment." In order for IHS to disclose patient data to a State or other health care registry pursuant to routine use no. 1:

- the registry must be established by a State, local or other "authorized" organization, and
- this registry must be part of a system that plans for, provides, or pays for health services, and
- the purpose of the IHS disclosure to the registry must be so that the registry may (a) plan for or provide health services, or (b) provide payment for health services, or (c) report the results of medical examination and treatment.

OGC suggests that although some registries may not appear to fulfill the health services' criteria of routine use no. 1. Most registries do report the results of medical examinations and, on that general basis, IHS may disclose information in accordance with routine use no. 1.

Routine Use VII: *"The IHS health care providers may disclose information from these records regarding the commission of crimes or the occurrence of communicable diseases, tumors, suspected child abuse, births, deaths, alcohol or drug abuse etc., as required by Federal law or regulation or State or local law or regulation of the jurisdiction in which the facility is located. Disclosure may be made to organizations as specified by the law or regulation, such as births and deaths to State or local health departments, and crimes to law enforcement agencies."* In order for IHS to disclose patient data to a State or other health care registry pursuant to routine use no. 7:

- the data regards the commission of crimes or the occurrence of communicable diseases, tumors, suspected child abuse, births, deaths, alcohol or drug abuse etc.

Appendix B: Transport of Immunization HL7 Transactions Over the Internet Using Secure HTTP, Ver. 1.0

Transport of Immunization HL7 transactions over the Internet Using Secure HTTP

Version 1.0
September 17, 2002

By The HL7 Immunization Registry Task Force sub group on HTTP message transport.

Joseph Rockmore – IBM Corporation
Andrey Yeatts – Scientific Technologies Corporation
Kevin Davidson – QS Technologies, Inc.

Transport of Immunization HL7 transactions over the Internet Using Secure HTTP

Introduction.....	iii
Privacy	iii
Authentication.....	iii
Transport Protocol for HL7 Messages over HTTP when using User ID/Password Authentication.....	iv
Transport Protocol for HL7 Messages over HTTP when using Digital Signatures	iv
Registry Server Lookup service.....	v
Batch Uploads via HTTP	vi
Reference Implementations	vi

Transport of Immunization HL7 transactions over the Internet Using Secure HTTP

Introduction

This document discusses conventions that may be used to transport Health Level Seven (HL7) messages over the Internet using Secure HTTP (HTTPS). It is the intent of sub group to use existing standards wherever possible.

Privacy

When transporting identifiable health information, the privacy of the information must be insured. Privacy may be insured by encrypting the message or transmitting the message over a secure channel. The HTTPS protocol, widely used for secure transactions in eCommerce, provides encryption and is recommended by this standard. The HTTPS protocol is defined in RFC 2660 (<http://www.ietf.org/rfc/rfc2660.txt>); however, we anticipate that commercial and public domain web servers and browsers will implement the protocol for these transactions and that immunization registry implementers will not be concerned with the details of the HTTPS protocol. If a secure channel (e.g. VPN or leased communications line) is available, the HTTP protocol may be used in lieu of HTTPS subject to local law and registry policy.

Authentication

Health information messages state important facts about personal information. Because of this, it is necessary to provide assurance of the identity of party asserting the facts in these messages. Authentication provides such assurance.

Two authentication methods are proposed.

1. User ID/Password. An immunization registry will provide each of its clients (other immunization registries and data providers) a User ID and a strong password. The client will present this User ID and password whenever sending transactions. Standards for User IDs and Passwords may be set by individual registries.
2. The HL7 message will be digitally signed using X.509 certificates and formatted according to the S/MIME standard. X.509 is a standard of the International Telecommunications Union.

Method 1 is considered primarily as a means whereby immunization data providers may authenticate with their state or regional registry. Method 2 is the preferred means for authentication between registries. However, either method is allowed in either situation subject to law and registry policy.

The sub group also recognizes that the complexity of implementing the digital signature may result in the User ID/Password method being the first deployed.

The S/MIME standard provides a structure to format messages that are digitally signed using an X.509 certificate. Encryption is an optional component of S/MIME. This

Transport of Immunization HL7 transactions over the Internet Using Secure HTTP

standard assumes that encryption through HTTPS or other secure channel will be used, and therefore use of the encryption facility of S/MIME is not required.

In order to use S/MIME, both the sender and the receiver must obtain X.509 digital certificates from agreed-upon Certificate Authority(s). The presentation of a message from a recognized Certificate Authority insures the identity of the sender and the integrity and non-deniability of the message. It does not, in and of itself, determine whether the sender is someone the registry should talk to; each registry implementation must develop a means of determining which presenters of valid certificates have permission to exchange messages with the registry.

This document does not address the issue of obtaining or distributing digital certificates, but we note that this is a significant issue.

Transport Protocol for HL7 Messages over HTTPS when using User ID/Password Authentication

When using User ID/Password Authentication, application programs will contact the registry server by issuing an HTTP POST transaction with the following data fields:

- **USERID** – This is the registry-assigned User ID. Implementations must support User ID's of at least 8 characters, including upper and lower case letters and digits. Case sensitivity of User ID is at the option of the implementing registry.
- **PASSWORD** – This is the registry-assigned Password for the User. Implementations must support Passwords of at least 8 characters, including upper and lower case letters and digits. Case sensitivity of the Password is at the option of the implementing registry.
- **FACILITYID** - The Facility ID is as defined in *Implementation Guide for Immunization Data Transactions using Version 2.3.1 of the Health Level Seven (HL7) Standard Protocol*, section 2.24.1.4 for the MSH Sending facility.
- **MESSAGEDATA** – The HL7 message as ASCII text. The message must begin with the character string “MSH”.

The response content to the HTTP POST will be the appropriate HL7 message as required by *Implementation Guide for Immunization Data Transactions using Version 2.3.1 of the Health Level Seven (HL7) Standard Protocol*. The HL7 message will not be encapsulated in any way.

Transport Protocol for HL7 Messages over HTTPS when using Digital Signatures

When using Digital Signatures for Authentication, application programs will contact the registry server by issuing an HTTP POST transaction with the following data fields:

Transport of Immunization HL7 transactions over the Internet Using Secure HTTP

- FACILITYID - The Facility ID is as defined in *Implementation Guide for Immunization Data Transactions using Version 2.3.1 of the Health Level Seven (HL7) Standard Protocol*, section 2.24.1.4 for the MSH Sending facility.
- MESSAGEDATA – The Message content will be the digitally signed HL7 message formatted in accordance S/MIME Version 2 specification available at <http://www.ietf.org/rfc/rfc2311.txt>.

The response content to the HTTP POST will be the appropriate HL7 message as required by *Implementation Guide for Immunization Data Transactions using Version 2.3.1 of the Health Level Seven (HL7) Standard*. Message content will be the digitally signed HL7 message formatted in accordance S/MIME Version [2](#).

HTTP Version and Recommended Headers

Where possible, HTTP version 1.1 (<http://www.ietf.org/rfc/rfc2616.txt>) should be used for all client messages.

When HTTP messages are sent, intervening servers may cache responses to improve overall network response. Because the messages discussed here are dynamic queries and updates, cached results are likely to be incorrect or out of date. HL7 query ids should be unique and so should not be cached, but to avoid any possible interaction with caching servers, the `no-cache` directives should be used in all HTTP headers. In HTTP version 1.1, these take the form:

```
Cache-control: no-cache
```

In version 1.0, the equivalent is:

```
Pragma: no-cache
```

Registry Server Lookup service

Both public key infrastructure and registry-to-registry communication require a lookup service to link registries with their public keys and http addresses.

Such a lookup (or directory) service should provide sufficient information to a client that the client could adequately determine the likely authoritative registry given address information in an HL7 query message or “other previous residence” address hints.

The information returned should include addresses for the HL7 HTTP server and human technical contact, and the public key used to communicate authentication messages to the registry.

The search information schema should include for each registry:

A printable name for the registry (ex: Arizona State Immunization Registry)

Transport of Immunization HL7 transactions over the Internet Using Secure HTTP

The country the covered by the registry's domain of service (ex: USA)

The state the registry's domain of service covers (ex: AZ)

If the registry is not authoritative for the entire state:

The list of counties the registry is authoritative for (ex: Maricopa)

If the registry is not authoritative for the entire county, or if there are cities outside the jurisdiction of any county for which the registry is authoritative:

The list of cities the registry is authoritative for (ex: Chandler, Mesa)

The returned data for a matching registry should include:

The HTTP/HTTPS URL for the HL7 service

The X509 public key for the service

A human technical contact email address

A human technical contact telephone

We recommend that an authority within the Immunization Registry community maintain a web site containing a directory of immunization registry HTTP servers by state, containing the URL, contact person, and phone number. The web page will be designed to be friendly to automated HTML parsers.

or

We recommend that an authority within the Immunization Registry set up an LDAP server to provide the URL, contact person, phone number and public key of each immunization registry HTTP server.

Batch Uploads via HTTPS

When batches of HL7 messages are sent via HTTP, they should be combined according to the HL7 Batch Protocol as described in by *Implementation Guide for Immunization Data Transactions using Version 2.3.1 of the Health Level Seven (HL7) Standard Protocol*. Batch uploads use the same specifications above, except that instead of the messages starting with "MSH", batches start with "FHS".

Reference Implementations

The working group proposed the creation of reference implementations demonstrating the protocols described herein. The purpose of the reference implementation is to provide examples that may be used as starting points by registry developers in implementing the protocols in this standard. The following are general principles for the reference implementations:

1. The reference implementations shall be open source.
2. The reference implementations should avoid, to the extent possible, registry-specific business logic, and should concentrate on the protocols.

Transport of Immunization HL7 transactions over the Internet Using Secure HTTP

3. The reference implementations should provide simple interfaces for authentication and message logging by external routines to be provided by the specific registry implementers.