RESOURCE AND PATIENT MANAGEMENT SYSTEM

Immunization Interface Management

(BYIM)

User Manual

Version 3.0
September 2020

Office of Information Technology
Division of Information Technology

Table of Contents

Revision History

Version	Date	Author	Section	Page Number	Summary of Change
3.0	September 2020	SESS	Entire Document	Entire Document	Initial version

Preface

This user manual contains information about the Resource and Patient Management System (RPMS) Immunization Interface Management (BYIM) application, also known as Immunization Data Exchange.

This manual:

- Introduces Immunization Interface Management (IIMM) and describes the functions and capabilities, for exchanging immunization data between a site's RPMS system and its State Immunization Information System (SIIS).
- Provides specific instructions for using IIMM options.
- Provides guidance and instructions for automating the immunization data exchange process between a local site and SIIS.

1.0 Introduction

Immunization, an established prevention practice, contributes to individual and community health by preventing infectious diseases in children and adults. Over the past decade, both the number of vaccines and the complexity of vaccine regimens have increased dramatically. Patients seek and obtain care and vaccinations from multiple healthcare resources, including county health departments, private providers and hospitals, and multiple Indian Health Service (IHS) Direct/Tribal/Urban (I/T/U) facilities.

The value and accuracy of vaccine forecasting and reporting features of the Resource and Patient Management System (RPMS) Immunization System application are dependent on complete and accurate vaccination histories in the local RPMS database. Although vaccination history is available to a local site (usually via a paper record), outside immunization information is not always entered into the local RPMS database.

Lack of access to or knowledge of full immunization information directly affects patient care, leading to inappropriate vaccination (incorrect dose timing or over-immunization) and misuse of vaccines, which are a valuable and costly resource.

The Centers for Disease Control and Prevention (CDC) has assisted in the development and use of vaccination registries at the state level. The RPMS Immunization Interface Management package (namespace: BYIM) improves patient care by enabling the exchange of vaccination data with state immunization registries.

1.1 About the Immunization Data Format

The data format used to exchange immunization information between a local site's RPMS and its State registry is the healthcare industry standard, Health Level Seven (HL7) Version 2.8. The HL7 standard dictates both content and format of the data to be exchanged. For more information, go to the HL7 Web site http://www.hl7.org/.

Sending HL7 messages to the state for inclusion in the state's immunization database meets the new requirements to share vaccination information with the state registry. More importantly at the local level, vaccines administered and reported to the state – but unknown to the local sites – are now sent back to the local site for inclusion in the local RPMS database.

1.1.1 Unsolicited Immunization Update

The files that send these to the state can be set to run automatically or can be manually generated. It is recommended that the messages be automatically generated and that the responses from the state be automatically processed.

The messages used are:

- Z22: Send Unsolicited Immunization Update (VXU) – This sends both Immunizations Administered and Immunization History to the SIIS. This is normally sent in batch mode at the end of the day but can also be manually generated.
- Z23: Return an Acknowledgement (ACK) – This can return either an Application Accept (AA), an Application Error (AE) or an Application Reject (AR).

1.1.2 State History and Forecast Request

This is a bi-directional interface that allows the IHS sites to send Evaluation Immunization and Forecast Requests and receive back the immunization history that is stored at the state and the state's recommended forecast.

This message is dependent on having an automatic electronic exchange setup with the SIIS, which is discussed in Section 2.0.

The message used are:

- Z44: Request Evaluated Immunization History and Forecast Query
- Z42: Return Evaluated History and Forecast
- Z33: Return an Acknowledgement with No Person Records – This will be returned if a matching patient is not found, too many matching patients were found (so the SIIS did not know which one to return), or an error occurred when processing the message.

There are four methods that can be used to request the state history and forecast. Note that these methods are not mutually exclusive and any or all methods can be utilized.

- Real-time request via the **Refresh State** button in the EHR Immunization Component.
- Real-time request via the new **Immunization Queries** option, described in Sections 3.7.1 and 3.7.5.
- Background job that sends requests for appointments that are scheduled for the current day. This is setup via a parameter discussed in Section 3.8.1.1.
- Trigger that sends a request when the patient is checked in. This is setup via a parameter discussed in Section 3.8.1.1.

1.2 Immunization Interface Management Process

Figure 1-1 displays the immunization data-exchange process with a fully automated process.

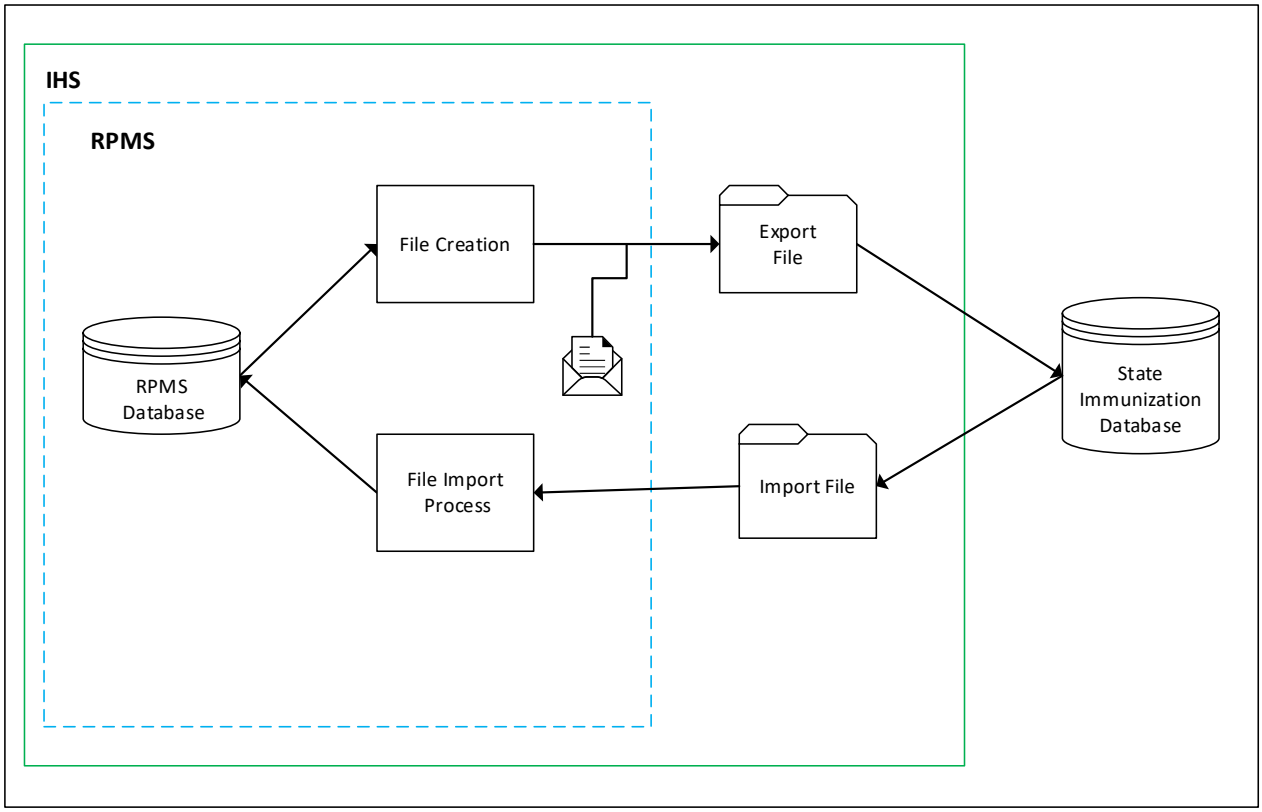

Figure 1-1: Immunization data exchange process

The **Start Immunization Data Export (IZDE)** option extracts immunization data from RPMS for a given date range, creates an HL7 immunization data export file, puts it in the site's secure export directory, and sends an email notification that the HL7 data export is ready.

If Simple Message Mover (SMM) is installed and operating, the transfer of HL7 immunization data files between the local site and the state registry can be automated.

2.0 Package Management

2.1 New Installation of BYIM

Before using any IIMM option, the site manager or other authorized person must do the following:

- Set up the BYIM EXPORT/IMPORT GROUP in MailMan for notifications.
- Create a local or network directories that will store the immunization export files.
- Set up the site parameters that specify the communication with your state SIISs.

2.1.1 Setup the BYIM EXPORT/IMPORT GROUP in MailMan

The site manager or other authorized person must set up the BYIM EXPORT/IMPORT GROUP in MailMan by adding the names of those individuals who should be notified whenever the following occurs:

- An HL7 immunization data export file is ready to be sent to the state registry.

Members of this mail group should include the following:

- An IT person tasked with monitoring/transmitting the immunization data files between the site and the state registry
- Clinical IZ staff member who performs the activities related to the IZDE option

2.1.2 Create Directories to Store the Export and Import Files

Specific directories should be created to store the export and import files. To be compliant with the Health Insurance Portability and Accountability Act (HIPAA), this directory must be in a secure area of the site's local computer.

2.1.3 Simple Message Mover

Transmitting the HL7 Immunization data files between the site and the state registry automatically requires SMM, which is a non-RPMS application. All IHS sites can install the SMM. However, it can only be utilized in states whose registries support secure data exchange via an HTTPS connection. This software must be installed and configured at your site by an authorized IT person. Instructions for installing SMM can be found on the https://www.ihs.gov/RPMS/PackageDocs/BYIM/BYIM_SimpleMessageMover.pdf website.

> **Note**: The directories specified by the Path for Outbound Messages and Inbound Messages parameters *must be the same* as the export/import directories used by the SMM.

2.1.4 Setting Site Parameters

There are multiple site parameters that control the communication with your SIISs and overall processing of the Immunization Data Exchange Package. See Section 3.8.1 on setting up these parameters.

2.2 Testing the Immunization Exchange

Before making Immunization Data Exchange fully functional, the Immunization exchange process should be tested using a smaller file and manually transmitted to the state.

- Create a test file.
- Transmit the test file to the SIIS.
- Receive and process the response.

2.2.1 Create a Test Immunization Data Export File

To create the initial file for testing, use the Create TEST Export File (IZTE) option to create the test file. Complete instructions for this option are included in Section 3.6.

MailMan sends an email notification to those names listed in the BYIM EXPORT/IMPORT GROUP that an immunization data file is in the Outbound Messages directory, ready to be sent to the state registry.

2.2.2 Data Export Filename Format

The filename format of HL7 immunization data export is izdata_<ASUFAC>_<YYYYMMDD>_<SSSSS>.dat where:

- **izdata** – Identifies the type of data as immunization data
- **ASUFAC** – Identifies the ASUFAC code of the site sending the data
- **YYYY** – Four-character year of file creation
- **MM** – Two-character month of file creation
- **DD** – Two-character day of file creation
- **SSSSS** – in $H seconds format

For example: izdata_000101_20061023_74158.dat

2.2.3 Transmit the Data File to the State Registry

Transmitting HL7 immunization data files between the site and the state registry can be done manually or automatically.

> **Note:** Check with both your site's IT person and your State Immunization Registry contact to verify the means of data exchange.

If SMM was installed and the connection with the SIIS is working, the files should automatically be sent to the SIIS. See the SMM documentation on how to know if SMM is working properly.

If you do not have an automatic connection with the SIIS, the files will need to be transmitted manually per the instruction with your SIIS. The HL7 immunization data files are located in secure directories, so manual transmission of HL7 immunization data can only be done by someone with the appropriate security clearance (usually an IT person) at your site.

The authorized person connects to the state registry via the internet using a state-registry supplied username and password. Then, the data file located in the site's export directory is uploaded to the state registry.

> **Note:** The login information used by IT personnel to access the state registry system is usually person specific. If personnel changes occur, the new IT person must contact the state registry to receive new access codes to avoid potential data security issues.

2.2.4 Process the Registry Data File returned by the State

If SMM was installed and the connection with the SIIS is working, the response files should automatically be returned to the SIIS. See the SMM documentation on how to know if SMM is working properly.

If you do not have an automatic connection with the SIIS and your SIIS has the functionality, the SIIS may have response files that can be imported into RPMS. Using the instruction provided by the SIIS, the file would be moved to the local directory created in Section 2.1.2 and specified in the BYIM setup.

If you do not have an automatic connection with the SIIS but your SIIS allows the site to manually transfer the file, the response files will need to be transferred manually to the to the local directory created in Section 2.1.2 and specified in the BYIM setup. The HL7 immunization data files are located in secure directories, so manual transmission of HL7 immunization data can only be done by someone with the appropriate security clearance (usually an IT person) at your site.

When the file is placed in the correct directory, it will be automatically imported into RPMS.

2.3 Creating the Initial Immunization File

2.3.1 Start Immunization Data Export

Once the process in Section 2.2 is working properly, the site should be ready to send the bulk of the immunizations to the SIIS. Sites export data for the following reasons:

- To make vaccine information available to other providers the patient may utilize
- To establish ownership of patients in order to get vaccine updates from the registry

> **Notes**: If the site has been manually entering immunizations into the state registry, the initial IZDE should not be needed. Please request IT Support to create a ticket to for the BYIM programmer/support person to set your system so the initial export of all immunizations for all patients ***will not*** be done.
>
> Prior to the initial export, it is highly recommended to use the parameter setup process to set the "Mark as 'HISTORIC' prior to...:" parameter to a date not more than 3–5 years from the date of the initial export. This will send all immunizations prior to the date specified as HISTORIC, which decreases the size of the export and avoids errors from older immunizations for which there may be missing data.

The **Start Immunization Data Export (IZDE)** option extracts immunization data from your site's RPMS database and creates an HL7 data export file (izdata) of the extracted data. The data export file is placed in the secure directory specified by the Path for Outbound Messages site parameter. The initial file can take a long time to complete (one to two hours or possibly more). Subsequent files will not take as long.

Please see Section 3.2 for complete instructions on the use of this option.

2.3.2 Checking the Immunization Data Export Status (IZCE)

The initial data export is quite large and can take many hours depending on the size of the patient population. Subsequent data extracts are completed quickly, in minutes rather than hours.

Please see Section 3.3 for complete instructions on the use of this option.

2.4 Automating the Immunization Data Exchange Process

2.4.1 Unsolicited Immunization Update

When you are assured of the accuracy and integrity of the immunization data exchanged between your site and the state registry, the process can be automated.

Considerations

- Both your site and your state immunization registry must be set up to handle electronic file transfers.
- Your site has an account with your state immunization registry.
- The local site's export/import directories must be located in a secure area.

The process for automating the automatic exchange of data with the SIIS is setting up the BYIM IZ AUTO EXPORT task. Using TaskMan, your site manager or other authorized person will need to schedule the **BYIM IZ AUTO EXPORT** option and specify the time and frequency to run. This task accomplishes the same functionality as the **Start Immunization Data Export (IZDE)** option except that it will run automatically and in the background.

MailMan sends an email notification to those names listed in the BYIM EXPORT/IMPORT GROUP that an immunization data file is in the Outbound Messages directory, ready to be sent to the state registry.

The data file of HL7 immunization data is transmitted from the Outbound Messages directory at your site to the state registry. The response file should automatically be returned and imported into RPMS.

2.4.2 State History and Forecast Request

Once the automatic exchange of information is set up, the bidirectional interface to request State History and Forecast Information from the SIIS can be setup. As previously discussed, the State History and Forecast can be requested in real-time or automated (or both). If you desire to automate the process that is done via the Auto Query Mode parameter in the Setup option discussed in Section 3.8.1.1.

2.5 Setting Up Communication with Additional SIISs

After the initial SIIS is setup, additional SIISs can be setup as desired. The process is similar to the setup of the initial SIIS documented above.

- Create directories to store the export and import files. The directory must be different than the directories used for the initial SIIS.
- If automating the connection to the additional SIIS, configure SMM for the additional SIIS.

- Do the BYIM configuration for the additional SIIS. This is done via the Define Additional Data Exchange Sites (IZAD) option in the **SET** menu as described in Section 3.8.2.
- Testing the connection.

3.0 Package Operation

3.1 Immunization Interface Management Menu

The **Immunization Interface Management Menu (IIMM)** provides a set of options that enable the user to prepare RPMS immunization data for export to the state registry.

3.1.1 Accessing the IIMM Main Menu

At the RPMS core menu prompt, type **BYIM** and press Enter. The IIMM Main Menu is displayed in Figure 3-1.

```
                        Immunization Data Exchange
                          2017 DEMO CLINIC CHIT

     BYIM VERSION: 3.0                  NEXT AUTO EXPORT: AUG 06@01:00
      HL7 VERSION: 2.5.1 R1.5 2016+     NEXT AUTO IMPORT: AUG 05@17:29:30
OUTPUT CONTROLLER: RUNNING              NEXT AUTO QUERY.: AUG 05@17:30
FORMAT CONTROLLER: RUNNING              NEXT AUTO PURGE.: AUG 06@01:00

   IZDE     Start Immunization Data Export
   IZCE     Check Immunization Data Export Status
   IZFS     File Statistics Report
   IZSI     Show Immunizations Exported for a Patient
   IZTE     Create TEST Export File
   IZQR     Immunization Queries
   SET      SETUP Options ...

 Select Immunization Interchange Management Menu Option:
```

Figure 3-1: IIMM main menu

3.1.1.1 IIMM Main Menu Header

The IIMM header displays:

- The BYIM Version Level
- The HL7 Version, which is dependent on the version that your SIIS uses and is configurable in the **Setup** option
- The status of the GIS OUTPUT CONTROLLER background process. If "NOT RUNNING – Contact IT support" displays, contact your IT support to restart the process so that the BYIM files are properly created.
- The status of the GIS FORMAT CONTROLLER background process. If "NOT RUNNING – Contact IT support" displays, contact your IT support to restart the process so that the BYIM files are properly created.
- The date/time the next automatic export of the batch VXU message.

- The date/time the next automatic import of messages will run.
- The date/time the next automatic query process will run.
- The date/time the next purge process will run.

3.1.1.2 IIMM Main Menu Options

Table 3-1 describes each of the IIMM options.

Table 3-1: IIMM options descriptions

Option	Description
Start Immunization Data Export (IZDE)	The Start Immunization Data Export menu option enables you to extract patient immunization data from RPMS, create an HL7 data export file, and place the file in a secure directory.
Check Immunization Data Export Status (IZCE)	The Check Immunization Data Export Status menu option enables you to check the progress of the IZDE process.
File Statistics Report (IZFS)	The File Statistics Report menu option enables you to generate a report that lists statistics related to patients and immunizations for each file that was created.
Show Immunizations Exported for a Patient (IZSI)	The Show Immunizations Exported for a Patient menu option enables you to print a report that lists all immunizations sent to the state registry for an individual patient to comply with HIPAA regulations.
Create TEST Export File (IZTE)	The Create TEST Export File menu option enables you to create a small file of real patients that will be used for initial data exchange testing between a site and its state immunization registry.
Immunization Queries (IZQR)	Various options use to send and review messages sent the site and the SIIS.
SETUP Options ... (SET)	The SETUP Options enables the BYIM manager to specify the site parameters, add additional export states and specify the SIIS assigned vaccine accountability codes.

3.2 Start Immunization Data Export (IZDE)

The **Start Immunization Data Export (IZDE)** option extracts immunization data from your site's RPMS database for a given date range and creates an HL7 data export file of the extracted data. The data export file is placed in the directory specified by the Path for Outbound Messages site parameter. It will also send an email notification that the HL7 data export is ready.

Considerations

- The export date range start date defaults to the day of the last export (if using point-of-care data entry, which will catch any patient and vaccines since the last export). However, if vaccines are entered by data entry staff and there is a delay, you will want to change this date to account for the three-day to three-week delay.
- The first time you perform this task, it may take a long time to complete (one to two hours or longer at large sites).
- When in doubt, go back and be overly inclusive. Sending the same data does not cause problems.
- If necessary, you can exit IZDE at the last prompt, "Requested Start Time," by typing a caret (^).

Notes: If the site has been manually entering immunizations into the state registry, the initial IZDE should not be needed. Please request IT Support to create a ticket to for the BYIM programmer/support person to set your system so the initial export of all immunizations for all patients ***will not*** be done.

Prior to the initial export, it is highly recommended to use the parameter setup process to set the "Mark as 'HISTORIC' prior to...:'" parameter to a date not more than 3–5 years from the date of the initial export. This will send all immunizations prior to the date specified as HISTORIC, which decreases the size of the export and avoids errors from older immunizations for which there may be missing data.

When this option is selected, a message displays, indicating that this process may take several minutes.

1. At the "Do you want to proceed?" prompt, type **Y** (yes) and press Enter. The following information displays:
   - The date of the last export
   - An indication of what data is being extracted based on the Ages to Export parameter in the **SETUP** option
2. At the "Export Immunizations starting on [today's date]" prompt, do one of the following:
   - Press Enter to accept the default export date, which is the current date.

- Enter a start date in MM/DD/YYYY format and press Enter. Specifying a start date allows you to go back to an earlier date, especially if there is doubt whether all past export files were properly transmitted, as well as to capture all children/vaccines from the specified date forward. Sending duplicate information does not create problems locally or at the state level, because both sides have de-duplication processes.

The process of extracting the immunization data from RPMS begins. The dots and slashes appearing on screen represent finding patient immunizations in the RPMS database and extracting the data.

3. At the "Requested Start Time" prompt, press Enter to accept the default start time **Now** or enter a different date/time that you want the process to start.

   The export file, **izdata_ASUFAC_YYYYMMDD_SSSSS.dat**, is created and placed in the directory specified by the Path for Outbound Messages site parameter.

   Figure 3-2 displays extracting and creating the HL7 immunization data export file.

```
Select Immunization Interchange Management Menu Option: IZDE <Enter>  Start
Immunization Data Export

Evaluation of immunizations of children 0-19 for export
to the State Immunization registry may take several minutes.

Do you want to proceed? NO// Y <Enter>  YES

The last Immunization export ran on JAN 24,2005 Children 19 and under were
born after JAN 24,1986

This export will include all children who have had a visit since the last
export ran or after the date you specify below.

You can enter another date if you want to run the export for another date
range.

Last Immunization export ran on JAN 24,2005 Children 19 and under were born
after JAN 24,1986

Export Immunizations starting on JAN 24,2005: JAN 24,2005// 01/01/2004
<Enter>.

.....................................................................
.....................................................................
.....................................................................
.....................................................................

Requested Start Time: NOW// <Enter> (JAN 24, 2005@13:20:30)

     The immunizations for 375 children 0-19 were evaluated in 2 seconds.

     The file 'izdata20070124.dat' will now be created in the HIPAA-
     compliant directory. This may take several minutes.
```

```
     It can be retrieved from this directory for transfer to the State
     registry.

Select Immunization Interchange Management Menu Option:
```

Figure 3-2: Example of extracting and creating the HL7 immunization data export file (IZDE)

3.3 Check Immunization Data Export Status (IZCE)

The **Check Immunization Data Export Status (IZCE)** menu option provides a quick look at the status of the data conversion and file creation process.

If the conversion is still in process, the message in Figure 3-3 displays. The number in parentheses after the status message will change each time you check the status.

- If the number increases, IZ is still searching and extracting immunization data from the RPMS database
- If the number decreases, IZ has found all the patients/vaccinations and is now converting the data into HL7 format

```
Immunization data export still in process. (349)
```

Figure 3-3: Data export message

When the conversion is complete, the message in Figure 3-4 displays. The export file (izdatayyyymmdd.dat) is now available in a secure directory of the local site's computer system.

```
The Immunization data export file is ready for transmission to the state
immunization registry.
```

Figure 3-4: Conversion complete message

3.4 File Statistics Report (IZFS)

After the export of immunization data files has been automated at your site, use the **File Statistics Report (IZFS)** menu option to get statistics on each file created.

Files can be selected by File Name or by Date Range.

At the "DEVICE" prompt, select the output device. The default is to send it to the HOME (screen) device, but a printer can be specified for a hard copy report.

This report lists the following information:

- File name, date, and type
- The following statistics:

- Number of patients
- Number of immunizations
- Number of no patient matches
- Number of new immunizations
- Number of added immunizations

Figure 3-5 displays an example of the File Statistics report (IZFS).

```
Select Immunization Interchange Management Menu Option: IZFS <Enter>  File Statistics
Report

   Select the FILE report option

   Select one of the following:

   1   File Name
   2   By Date range

Enter response: 2

Beginning Date FILE STATISTICS Report: JUL 19,2017// 7/12/2017

Ending Date FILE STATISTICS Report: JUL 19,2017//

DEVICE: HOME//  Virtual

File Status Report  Report Date: 07/19/2017

   IMP/EXP    Pat-    Imuni- NO Pat New IMS
File  Date    Type    ients  zations    Match  Imms   Added
------------ ----------    -------    ------ -----

File Name Prefix: izdata_232101_

20170712_34264.dat 07/12/2017    EXPORT 40  197
20170712_38453.dat 07/12/2017    EXPORT 40  197
20170712_63874.dat 07/12/2017    EXPORT 2   41

Press <ENTER> to continue or '^' to exit...:
```

Figure 3-5: Example of the File Statistics report (IZFS)

3.5 Show Immunizations Exported for a Patient (IZSI)

The **Show Immunizations Exported for a Patient (IZSI)** option enables facilities to comply with HIPAA regulations by printing a report that lists all immunizations sent to the registry for an individual patient.

> **Note:** This report can be generated only for patients who have had information exported previously to their state immunization registry.

1. At the “Enter Name, HRN, or DOB” prompt, type the Patient Name (last name first), a health record number (HRN), or a date of birth (DOB) and press Enter.
2. At the “DEVICE” prompt, select the output device. The default is to send it to the HOME (screen) device, but a printer can be specified for a hard-copy report.

Figure 3-6 displays the **Immunization Interchange Management Menu**.

```
Select Immunization Interchange Management Menu Option: EXP <Enter> Enter
Name, HRN, or DOB: PATIENT, A <Enter>

DEVICE: HOME//  Virtual

Immunization Export summary for:
PATIENT,A DOB: 05/12/1930  HRN: 748526

     Export Date  Immunization          Admin Date
     -----------  --------------------  -----------
     08/25/2006   TD (ADULT)            03/01/1988
V IMMUNIZATION has been edited or deleted
     08/27/2006   TD (ADULT)            03/01/1988
V IMMUNIZATION has been edited or deleted
     08/28/2006   TD (ADULT)            03/01/1988
V IMMUNIZATION has been edited or deleted
     08/29/2006   TD (ADULT)            03/01/1988
V IMMUNIZATION has been edited or deleted

Press <ENTER> to continue or '^' to exit...:
```

Figure 3-6: Example of report of immunizations exported to the state registry for a patient (EXP)

3.6 Create TEST Export File (IZTE) option

This option is used to create a test export file. It allows the flexibility to determine what patients should be sent in the export file.

The first prompt is whether you want to create an export file for a random group of patients or select the patients for export.

1. If the **Selected Patients** option is chosen:
   a. The user will then be prompted to enter a list of patients to export. Multiple patients can be selected.
   b. A message with the selected patients is shown.
   c. At the "Proceed with export of selected patients?", type **YES** to continue.
2. If the **Random Patients** option is selected.
   a. The user is prompted for number of patients (1–1000). The default is 10.
   b. The user is then prompted to select one or more of the following:

i. Specify the start date for immunizations to include. If selected, the user will be prompted for the Start Date they want to use.

ii. Exclude HISTORIC immunizations. If selected, the user will be prompted whether to include or exclude Historic Immunizations.

iii. Exclude PREVIOUSLY EXPORTED immunizations. If selected, the user will be prompted whether to include or exclude previously exported immunizations.

c. A message displays with the selection criteria.

d. At the "Proceed with TEST export?" prompt, enter **YES** to continue.

3. At the "Requested Start Time" prompt, press Enter to create the file now.

The system creates an export file of immunizations based on the parameters above and based on the Ages to Export parameter in the **SETUP** option. When the process is complete, the system displays the following:

- The number of immunizations that were evaluated.
- The name and location of the export file.

Figure 3-7 displays an example of a test immunization data export file.

```
Select Immunization Interchange Management Menu Option: TEST <Enter>
Create TEST Export File
         Select group of patients for TEST export

      Select one of the following:

           1    Random group of patients
           2    Select patients for test export

Which group of patients: Random group of patients//

           TEST export option
           An export file will be created for Patients of all ages.

Enter the number of patients to include in the test export:(1-1000): 10// 1

           Default TEST export criteria

           TEST Export Criteria:

Start date:

Only administered and never exported immunizations will be included in the
test export.

      1.   Specify start date for immunizations to include
      2.   Exclude HISTORIC immunizations
      3.   Exclude PREVIOUSLY EXPORTED immunizations

Select all criteria you want to set:    (1-3): 1-3

Select start date for the TEST export: 7/30/2013
```

```
Exclude HISTORIC immunizations? YES// NO

Exclude PREVIOUSLY EXPORTED immunizations? YES// NO

TEST Export Criteria:

Start date: JUL 30,2013

Administered and historic and new and previously exported immunizations
will be included in the test export.

Proceed with test export of 1 patients? NO// YES/ Requested Start Time:
NOW// (JUL 19, 2017@13:06:33)

27 immunizations for 1 Patients 0-99 were evaluated in 0 minutes, 0
seconds.

The file 'izdata_232101_20170719_47189_test.dat' will now be created in the
'/local/hl7immunizationDataExport/' directory. This may take several
minutes.

It can be retrieved from this directory for transfer to the State registry.

Press <ENTER> to continue or '^' to exit...: <Enter>
```

Figure 3-7: Example of a Test Immunization Data Export file

3.7 Immunization Queries (IZQR)

The **Immunization Queries (IZQR)** option provides additional functionality to send data to the SIISs. It also includes the ability to see the data that was sent to the state and the responses received, which could be especially helpful for debugging purposes.

Figure 3-8 shows the functionality available with this option.

```
          Immunization Query Options - Version: 2.5.1 R1.5 2016+

     Select one of the following:

          1         Request Patient Imm History and Forecast
          2         Send Patient Immunizations
          3         Review Query or VXU Response
          4         Review Query or VXU Sent
          5         Send Scheduled Appt Queries
```

Figure 3-8: Functionality available in the Immunization Queries option

3.7.1 Request Patient Imm History and Forecast

The **Request Patient Immunization History/Forecast** option allows the user to send an Immunization History and Forecast request (Z44) for one or more patients. For each patient selected, a request will be sent to each SIIS that is configured for the site. Within a few seconds, the response from the SIIS should be received and stored. The response can then be displayed either in the EHR Immunization component or in the Review Query or VXU Response functionality included in this option.

Figure 3-9 has an example of requesting the patient immunization history and forecast via this option.

```
Select patient(s) to send to the State Immunization Registry

Select patient:
  PATIENT,DEMO               M 01-18-1990 XXX-XX-0568   CIM 101657

    1               PATIENT,DEMO

Select another patient:


A 'Request for Evaluated Imm History and Forecast' will be sent for:

    1               PATIENT,DEMO

Do you want to proceed? YES//

Please stand by. This may take a couple of seconds...

Query being sent for: PATIENT,DEMO

Query for : PATIENT,DEMO
     being sent to: ARIZONA
     QUERY Message ID: IHS-927 for PATIENT,DEMO
     and can be used to look up the responses from:
          ARIZONA
```

Figure 3-9: Example of the Request Patient Imm History and Forecast functionality

3.7.2 Send Patient Immunizations

The **Send Patient Immunizations** option allows the user to send an Unsolicited Vaccine Record Update (Z22-VXU) message for one or more patients. The option also allows user to send all vaccines for the patient or only the new, modified, or deleted vaccines that have not already been sent. For each patient selected, a VXU message will be sent to each SIIS that is configured for the site.

Figure 3-10 has an example of requesting the patient immunization history and forecast via this option.

```
Which immunizations should be included:
```

```
     Select one of the following:

          1     NEW/EDITED Immunizations (not previously exported)
          2     ALL Immunizations for exported patient(s)

Send NEW or ALL Immunizations: NEW/EDITED Immunizations// 2  ALL
Immunizations for exported patient(s)

Select patient(s) to send to the State Immunization Registry

Select patient:
  PATIENT,DEMO              M 01-18-1990 XXX-XX-0568   CIM 101657

    1               PATIENT,DEMO

Select another patient:

An 'Unsolicited Vaccine Record Update (VXU)' will be sent for:

    1               PATIENT,DEMO

Do you want to proceed? YES//

Please stand by.  This may take a couple of seconds...


Immunization record for: PATIENT,DEMO
          being sent to: ARIZONA
```

Figure 3-10: Example of the Send Patient Immunizations functionality

3.7.3 Review Query or VXU Response

> **Note**: Due to a patient lookup issue, do not use this option until the release of BYIM v3.0 patch 1.

The **Review Query or VXU Response** option allows the user to review the response returned by the SIIS, whether the response is an acknowledgement to an Unsolicited Vaccine Record Update (VXU) message or a response to an Immunization History/Forecast request. The user has the option to display only the Immunization Information only or to display the complete HL7 message.

Figure 3-11 has an example of running the Review Query or VXU Response and the type of data returned when the Immunization Information Only view is requested.

```
     Select one of the following:

          1         Immunization Information Only
          2         HL7 Message Content

Which display option: Immunization Information Only//


Response received              Date/State File Name/Message ID
```

```
------------------------------ ---------- ------------------------------------
PATIENT,DEMO S     (M)         06/11/2020 izrt_qbp_911_6_20200611_220349.dat
DOB: 02/14/1950  HRN: 648286   COLORADO   IHS-999

Response ID: (1826)     Query or VXU ID: (1714)
-------------------------------------------------------------------------------
Patient,Demo S                 02/14/1950 M HRN:
------------------------------ ---------- - -----------
  CVX VACCINE ADM DATE AGE    LOCATION REACTION VOL SITE LOT   MAN VALID STATUS
- --- ------- -------- ------ -------- -------- --- --- ------ --- ----- ----
  140 FLU-IIV 20151029 65 yrs OTHER             .5             bio Y     COMPLE

Press <ENTER> to continue or '^' to exit...:

Patient,Demo S                 02/14/1950 M HRN:
------------------------------ ---------- - -----------
    IMMUNIZATION FORECAST:
CVX VACCINE     STATUS DUE        EARLIEST   LATEST     STANDARD
--- ----------- ------ ---------- ---------- ---------- --------
152 PCV-NOS            01/01/2060 01/01/2060            ACIP
 88 FLU,NOS            09/01/2016 09/01/2016            ACIP
  3 MMR                01/01/1996 01/01/1996            ACIP
 21 VARICELLA          01/01/1996 01/01/1996            ACIP
115 Tdap               01/01/2002 01/01/2002            ACIP

Press <ENTER> to continue or '^' to exit...:
```

Figure 3-11: Example of the Review Query or VXU Response functionality

3.7.4 Review Query or VXU Sent

> **Note**: Due to a patient lookup issue, do not use this option until the release of BYIM v3.0 patch 1.

The **Review Query or VXU Sent** option allows the user to review the message sent to the SIIS, whether an Unsolicited Vaccine Record Update (VXU) message or an Immunization History and Forecast Query request. The user has the option to display the immunization information only or to display the complete HL7 message.

Figure 3-13 has an example of running the Review Query or VXU Response and the type of data returned when the Immunization Information Only view is requested.

```
Select Original Query or VXU sent
Select Patient, VXU Date or Message ID: PATEINT,DEMO
izrt_vxu_26880_3_20200716_223916.dat     PATIENT,DEMO     Jul 16,2020@22:39:16
IHS-112323     ARIZONA

     Select one of the following:
          1         Immunization Information Only
          2         HL7 Message Content
Which display option: Immunization Information Only//

HL7 message sent:              Date/State File Name/Message ID
------------------------------ ---------- ------------------------------------
PATIENT,DEMO  (F)              07/16/2020 izrt_vxu_26880_3_20200716_223916.da
```

```
DOB: 03/17/1995  HRN: 7120     ARIZONA    IHS-112323
Query or VXU (1094)
------------------------------------------------------------------------
PATIENT,DEMO                   03/17/1995 F HRN: 007120
------------------------------ ---------- - -----------
  CVX VACCINE ADM DATE AGE    LOCATION REACTION VOL SITE LOT   MAN VALID STATUS
- --- ------- -------- ------ -------- -------- --- --- ------ --- ----- ----
S 121 ZOS-Liv 20150317 20 yrs 2020 DEM          999                     CP
Press <ENTER> to continue or '^' to exit...:
```

Figure 3-12: Example of the Review Query or VXU Sent functionality – Immunization Information Only content

Figure 3-13 has an example of running the Review Query or VXU Response and the type of data returned when the HL Message Content view is requested.

```
         Select Original Query or VXU sent

Select Patient, VXU or Query Date or Message ID:
izrt_qbp_911_6_20200611_220349.dat     PATIENT,DEMO S        Jun 11,2020@22:03:49
IHS-999     COLORADO


    Select one of the following:

         1         Immunization Information Only
         2         HL7 Message Content

Which display option: Immunization Information Only//


HL7 Message sent               Date/State File Name/Message ID
------------------------------ ---------- ----------------------------------
PATIENT,DEMO S     (M)         06/11/2020 izrt_qbp_911_6_20200611_220349.dat
DOB: 02/14/1950  HRN: 999986   COLORADO   IHS-999

Query or VXU ID: (1714)
------------------------------------------------------------------------
MSH|^~\&|NISTEHRAPP|NISTEHRFAC|NISTIISAPP|NISTIISFAC|20200611220348-
0700||QBP^Q11^QBP_Q11|IHS-
542|P|2.5.1|||ER|AL|||||Z44^CDCPHINVS|NISTEHRFAC^^^^^ANON^ANON^^^1
00-6482|NISTIISFAC^^^^^RPMS^XX^^^100-3322
QPD|Z44^Request Evaluated History and Forecast^CDCPHINVS|IHS-542|648286^^^NIST-MPI-
1^MR~123456789^^^MEDICARE^MC|Demo^Patient^S^^^^L|
Bell^Mother^^^^^M|19500214|M|1642 Bear Run^^Bozeman^MT^59715^USA^P|^PRN^PH^^^
406^5552020|N|1||
RCP|I|1^RD&records&HL70126|||||

Press <ENTER> to continue or '^' to exit...:
```

Figure 3-13: Example of the Review Query or VXU Sent functionality – HL7 message content

3.7.5 Send Scheduled Appt Queries

The **Send Scheduled Appt Queries** option allows the user to send Immunization History and Forecast Query (Z44) request for every patient that has a scheduled appointment or check-in on the date selected by the user. This will default to the value in the Auto Query Mode parameter if it is set. Otherwise, the user can select **Schedule appointments only**, **Check-ins only**, and **Both scheduled appts and check-ins**.

The user is then allowed to select the date of the scheduled appointments or check-ins. Figure 3-14 has an example of running the **Send Scheduled Appt Queries** option.

```
          Auto Query Mode is not set.
          To Set the mode for the system:

          Use the BYIM Main Menu 'Set' option
          then select: 'SET   SET UP Immunization Data Exchange Parameters
          then select: '1   Edit Parameters for (name of state)'
          and go to and set the 'Auto Query Mode' parameter.

          You can also select one of the choices below
          to run the auto query one time.



     Select one of the following:

          1         Scheduled appointments only
          2         Check-ins only
          3         Both Scheduled appts and Check-ins

Which auto query mode: 1  Scheduled appointments only

          Select a date for which to send queries for:
          Scheduled appointments only


     Date for Appointment Queries:  T

          Queries will be sent for all patients who have
          Scheduled appointments only on AUG 6,2020

Press <ENTER> to continue or '^' to exit...:
```

Figure 3-14: Example of the Send Scheduled Appt Queries functionality

3.8 SETUP Options ... (SET) menu

The **SETUP Options** menu allows SIIS-specific information to be entered. It has functionality that allows the entry of state specific parameters for multiple SIISs.

```
                    Immunization Data Exchange
                      2017 DEMO CLINIC CHIT
```

```
       BYIM VERSION 3.0                  NEXT AUTO EXPORT: AUG 06@01:00
        HL7 VERSION 2.5.1 R1.5 2016+     NEXT AUTO IMPORT: AUG 05@17:29:30
   OUTPUT CONTROLLER: RUNNING            NEXT AUTO QUERY.: AUG 05@17:30
   FORMAT CONTROLLER: RUNNING            NEXT AUTO PURGE.: AUG 06@01:00


         SET    SET UP Immunization Data Exchange Parameters
         IZAD   Define Additional Data Exchange Sites
         IZIS   Add/Edit IIS Assigned Vaccine Inventory Codes

Select SETUP Options Option:
```

Figure 3-15: Example of the File SETUP submenu

3.8.1 Set Up Data Exchange Site Parameters (SET)

The user is given the option to edit parameters for the primary export state, add specific facilities for the primary state export, or add IIS codes to the primary export state (Figure 3-16).

```
 State: 2017 DEMO CLINIC CHIT
Path...: g:\smm\asiis\request\                        Ages...: 18 AND UNDER
MSH-3.1: PRMS        MSH-3.2:                                  MSH-3.3:
MSH-4.1: IRMS 63027  MSH-4.2:                                  MSH-4.3:
MSH-5.1: ASIIS       MSH-5.2:                                  MSH-5.3:
MSH-6.1: ASIIS       MSH-6.2:           MSH-6.3:               Version:
2.5.1
MSH21.1: Z22         MSH21.2: CDCPHINVS
MSH22.1: NISTEHRFAC  MSH22.6: RPMS      MSH22.7: XX    MSH22.10: 100-6482
MSH23.1: NISTIISFAC  MSH23.6: RPMS      MSH23.7: XX    MSH23.10: 100-3322
PID11.7: PERMANENT   RXA-5.1: NDC ONLY                 RXA-6.1 :
File Extension......: dat               Protection Indicator: PI NOT NEEDED
Include/Exclude SSN.: EXCLUDE SSN       Include Insurance...: NO
Include/Exclude PV1.: EXCLUDE PV1       Auto Query Mode.....:
Purge Messages after: 90 days           Exchange State......: ARIZONA
Barcode/Vac type Seg: VIS BARCODE


     Select one of the following:

Select one of the following:

      1   Edit parameters for (primary export state)
      2   Add specific FACILITY(IES) for (primary export state) export
      3   Add (primary export state) specific IIS code(s)
```

Figure 3-16: Primary state options

3.8.1.1 Edit Parameters for (Primary Export State)

This option allows a user to set up the specific data exchange parameters required by the primary export state as well as some overall BYIM system parameters. You will need to work with your specific State Immunization Information Systems (SIISs) to determine the appropriate values that your SIISs want entered in almost all of these fields. The values that can be modified are:

- **Path for Outbound Messages**: The local or network directory in which the site's HL7 immunization data files are located. If SMM is being used to transfer these files to the state registry, the location specified here must be the same as the location monitored by SMM.

  Important: To be HIPAA compliant, this directory must be in a secure area of the site's local computer.

- **Path for Inbound Messages:** The local or network directory in which the state's HL7 immunization data files are located. If SMM is being used to transfer the state immunization files to the site, the location specified here must be the same as the location used by SMM.

  Important: To be HIPAA compliant, this directory must be in a secure area of the site's local computer.

- **Ages to Export**: Specifies the immunization data age groups to include in the data export files. Possible values are below with the default value being '2: All ages.'
  - 0: 18 years and under (default)
  - 1: Under 19 years and over 64 years
  - 2: All ages
- **Sending Application MSH-3.1**.: This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then 'RPMS' will be sent in this HL7 element.
- **Sending Application MSH-3.2.:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing will be sent in this HL7 element.
- **Sending Application MSH-3.3.:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing will be sent in this HL7 element.
- **Sending Facility MSH-4.1.:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then 'RPMS' will be sent in this HL7 element.

- **Sending Facility MSH-4.2.:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing will be sent in this HL7 element.
- **Sending Facility MSH-4.3.:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing will be sent in this HL7 element.
- **Receiving Application MSH-5.1.:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing will be sent in this HL7 element.
- **Receiving Application MSH-5.2.:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing will be sent in this HL7 element.
- **Receiving Application MSH-5.3.:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing will be sent in this HL7 element.
- **Receiving Facility MSH-6.1:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing will be sent in this HL7 element.
- **Receiving Facility MSH-6.2:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing will be sent in this HL7 element.
- **Receiving IIS Facility MSH-6.3:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing will be sent in this HL7 element.
- **Flag TEST messages T MSH-11..:** This parameter allows the flagging of messages as Test or Production messages. Possible values are below with the default value being 'P: Production'.
  - P: Production
  - T: Test
- **HL7 Version in use MSH-12..:** This the HL7 message version used by the state. The possible values are below with the default value being '4: 2.5.1 R1.5 2016+'.
  - 1: 2.3.1
  - 2: 2.4
  - 3: 2.5.1 R1.5 <2016
  - 4: 2.5.1 R1.5 2016+

- **Profile Identifier MSH-21.1:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing will be sent in this HL7 element.
- **Profile Identifier MSH-21.2:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing will be sent in this HL7 element.
- **Sending Org Name MSH-22.1:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing is placed in the HL7 component.
- **Sending Org Auth MSH-22.6:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing is placed in the HL7 component.
- **Sending Org Type Code MSH-22.7:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing is placed in the HL7 component.
- **Sending Org ID MSH-22.10:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing is placed in the HL7 component.
- **Receiving Org Name MSH-23.1:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing is placed in the HL7 component.
- **Receiving Org Auth MSH-23.6:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing is placed in the HL7 component.
- **Receiving Org Type Cd MSH-23.7:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing is placed in the HL7 component.
- **Receiving Org ID MSH-23.10:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing is placed in the HL7 component.
- **Primary Facility Name PD1-3.2.:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing will be sent in this HL7 element.
- **Primary Facility ID PD1-3.3.:** This is the value that SIIS specifies should be placed in this HL7 fields. If not specified, then nothing will be sent in this HL7 element.
- **CVX or NDC Code for RXA-5.1:** Allows the choice of which codeset should be sent in the RXA-5 field. The possible values are below with the default value being NDC ONLY.

  - 0: CVX ONLY
  - 1: CPT ONLY
  - 2: CVX AND CPT
  - 3: NDC ONLY
- **Value for blank volume RXA-6.1:** This parameter indicates the default value used in the RXA-6.1 component when there is no volume specified in the RPMS immunization data.
- **File extension (dat or hl7)...:** Specify the file extension of the export files. The possible values are below with the default value being ‘dat’.
  - dat
  - hl7
- **Protection Indicator Enforced.:** The possible values are below with the default value being PI NOT NEEDED.
  - 0: PI NOT NEEDED
  - 1: PI MUST BE ON FILE
- **Mark as 'HISTORIC' prior to...:** If a date is specified in this parameter, all immunization prior to that date will be sent as historic immunizations.
- **Exclude Patient's SSN.....:** This parameter indicates whether the patient SNN should be sent to the SIIS. The possible values are below with the default value being '1: INCLUDE SSN'.
  - 1: EXCLUDE SSN
  - 0: INCLUDE SSN
- **Include Insurance Segments....:** This parameter indicates whether the Insurance segment (INS) should be send the HL7 message sent to the SIIS. The possible values are below with the default value being '0: NO'.
  - 0: NO
  - 1: YES
- **Exclude PV1 Segment.....:** This parameter indicates whether the Patient Visit segment (PV1) should be send the HL7 message sent to the SIIS The possible values are below with the default value being '0: EXCLUDE PV1'.
  - 0: EXCLUDE PV1
  - 1: INCLUDE PV1

- **Auto Query Mode.....:** This parameter indicates the method used to automatically create the Evaluated History and Forecast request. If the sites exchange data with multiple SIISs, this parameter will be used by all of the SIISs. The possible values are below with the default value being no option is set. Note that this value does not need to be set in order to get State History and Forecast information as it can be obtained using the **STATE REFRESH** button in the EHR Immunization component or the functionality in the **Immunization Queries** (IZQR) option.
  - **1: SCH'D APPTS ONLY**. This setting will send requests to the SIIS for appointments scheduled for that day. The process runs every five minutes so it will send most of the requests early in the morning, but it will also send requests if new appointments are created later for the same day.
  - **2: CHECK-IN ONLY**. This setting will send requests to your SIISs as each patient is checked in.
  - **3: SCH'D AND CHECK-IN**. This setting will do both of the above.
- **Purge HL7 Message after ? days:** A copy of all HL7 message sent to and received from the SIISs are stored in RPMS for viewing and debugging. In order to manage disk space utilization, these messages are purged based on the number of days set in this parameter. If your site exchanges data with multiple SIISs, this parameter will be used by all of the SIISs. The number of days can be between 90 and 999 with the default being 90 days.
- **Use VIS Barcode or NOS SEGS...:** This parameter determines whether the Vaccine Information Statement (VIS) information or the Not Otherwise Specified (NOS) Document Type data is sent in the OBX segments. You will need to work with your specific SIISs to determine the appropriate value that should be used in this parameter. The possible values are below. Note that if the parameter is not set, the default values sent in the OBX segment will be the VIS barcode data.
  - 0: VIS BARCODE
  - 1: NOS DOC TYPE
- **State site exchanges with.....:** Enter the state name for the SIIS. Valid values come from the STATE (#5) file.
- **Organization ID 1.....:** This parameter is intended for future use.
- **Organization ID 2.....:** This parameter is intended for future use.
- **Organization ID 3.....:** This parameter is intended for future use.
- **Organization ID 4.....:** This parameter is intended for future use.
- **Organization ID 5.....:** This parameter is intended for future use.

Figure 3-17 displays an example of setting the immunization data exchange parameters for the primary state.

```
Which ADDITIONAL export function for ARIZONA: 1  Edit parameters for
ARIZONA


Path for OUTBOUND Messages....: g:\smm\asiis\request\
          Replace
Path for INBOUND Messages.....: g:\smm\asiis\response\
          Replace
Ages to Export................: 18 AND UNDER//
Sending Application   MSH-3.1.: PRMS//
Sending Application   MSH-3.2.:
Sending Application   MSH-3.3.:
Sending Facility      MSH-4.1.: IRMS 63027//
Sending Facility      MSH-4.2.:
Sending Facility      MSH-4.3.:
Receiving Application MSH-5.1.: ASIIS//
Receiving Application MSH-5.2.:
Receiving Application MSH-5.3.:
Receiving Facility     MSH-6.1: ASIIS//
Receiving Facility     MSH-6.2:
Receiving IIS Facility MSH-6.3:
Flag TEST messages T  MSH-11..: Production//
HL7 Version in use    MSH-12..: 2.5.1 R1.5 2016+//
Profile Identifier    MSH-21.1: Z22//
Profile Identifier    MSH-21.2: CDCPHINVS//
Sending Org Name      MSH-22.1: NISTEHRFAC//
Sending Org Auth      MSH-22.6: RPMS//
Sending Org Type Code MSH-22.7: XX//
Sending Org ID       MSH-22.10: 100-6482//
Receiving Org Name    MSH-23.1: NISTIISFAC//
Receiving Org Auth    MSH-23.6: RPMS//
Receiving Org Type Cd MSH-23.7: XX//
Receiving Org ID     MSH-23.10: 100-3322//
Primary Facility Name PD1-3.2.:
Primary Facility ID   PD1-3.3.:
CVX or NDC Code for    RXA-5.1: NDC ONLY//
Value for blank volume RXA-6.1:
File extension (dat or hl7)...: dat//
Protection Indicator Enforced.: PI NOT NEEDED//
Mark as 'HISTORIC' prior to...:
Exclude Patient's SSN.........: EXCLUDE SSN//
Include Insurance Segments....: NO//
Exclude PV1 Segment...........: EXCLUDE PV1//
Auto Query Mode...............:
Purge HL7 Message after ? days: 90//
Use VIS Barcode or NOS SEGS...: VIS BARCODE//
State site exchanges with.....: ARIZONA//
Organization ID 1.............:
Organization ID 2.............:
Organization ID 3.............:
Organization ID 4.............:
Organization ID 5.............:
```

Figure 3-17: Example of the immunization data exchange parameters (SET)

3.8.1.2 Add Specific Facility(ies) for (Primary Export State) Export

This menu option presents the following selections:

```
Which ADDITIONAL export function for ARIZONA: 2  Add specific FACILITY(IES)
for


          Facility(ies) to include in the
     No.  ARIZONA state export                    IIS Code
     ---  ---------------------------------------  --------------------



     Select one of the following:

          1         Select Facility to include in the export
          2         Remove Facility from the export
```

Figure 3-18: Example of Add specific FACILITY(IES) prompt

- **Select Facility to include in the export**

  Select option **1** to add facilities to a specific state export. A list of available facilities displays. When you select a facility, the following options display:

  – **Edit IIS Facility Code for**
  – **State IIS Facility Code**

```
Which option: 1  Select Facility to include in the export

          Facility(ies) to include in the
     No.  NEW MEXICO Additional state export      NEW MEXICO IIS Code
     ---  ---------------------------------------  --------------------
     1    2013 DEMO HOSPITAL   (4711)              NM_TEST_4711

Select another Facility to include in the export: CIMARRON HOSPITAL
TUCSON      01

Edit IIS Facility Code for: CIMARRON HOSPITAL
State IIS Facility Code...: NM_CIM_4585//

          Facility(ies) to include in the
     No.  NEW MEXICO Additional state export      NEW MEXICO IIS Code
     ---  ---------------------------------------  --------------------
     1    CIMARRON HOSPITAL  (4585)               NM_CIM_4585
     2    2013 DEMO HOSPITAL (4711)               NM_TEST_4711

Select another Facility to include in the export:
```

Figure 3-19: Add additional facility

- **Remove Facility from the export**

  Select option 2 to remove a facility from the state export. When you select a facility to remove from the list of currently assigned facilities, a new list displays reflecting the removal.

3.8.1.3 Add (Primary Export State) Specific IIS Code(s)

Select this menu option to add, edit, or delete an IIS-assigned vaccine inventory location code for facilities configured to export to the primary export state.

The selection options are as follows:

1. **Edit a listed Code**
2. **Add IIS Code for another Facility**
3. **Delete IIS Code for a Facility**

```
ARIZONA IIS Assigned Vaccine Inventory Location Code

          NO.  Facility                              IIS Code
          ---  --------------------------            --------------------
          1    2013 DEMO CLINIC (IEN 2907)           SIIDEMOCLINIC
          2    2013 DEMO HOSPITAL (IEN 2906)         UNMH
          3    2013 DEMO TRIBAL HOSPITAL (IEN 2908)  ISSTRIBAL

     Select one of the following:

          1         Edit a listed Code
          2         Add IIS Code for another Facility
          3         Delete IIS Code for a Facility

Enter response:
```

Figure 3-20: IIS code options

3.8.2 Define Additional Data Exchange Sites (IZAD)

This option allows secondary SIISs to be added to as additional exchanges. Each state may have specific values that it wants to have defined for the data that passes between RPMS and the state. This option allows those values to be setup for each state. Please see Section 3.8.1.1 for a complete listing and explanation of these values.

Figure 3-21 displays options on the Define Additional Data Exchange Sites screen.

```
                Additional EXPORT/IMPORT Site Directories

      NUM       SITE/STATE
      ----      ---------------------------------------------

       1        COLORADO
                   OUTBOUND: d:\temp\SMM\colorado\requests
                   INBOUND: d:\temp\SMM\colorado\responses
       2        NEW MEXICO
                   OUTBOUND: d:\temp\SMM\new_mexico\requests
                   INBOUND: d:\temp\SMM\new_mexico\responses

      Select one of the following:

         1      Edit site
```

```
          2      Add site
          3      Delete site

   Enter response: 1   Edit site

   Select site number: (1-2): 2

  State: NEW MEXICO
Path...: g:\smm\nmsiis\request\                          Ages...: ALL AGES
MSH-3.1: nmsiis      MSH-3.2:                                  MSH-3.3:
MSH-4.1: NMSIIS      MSH-4.2: nmsiis                           MSH-4.3:
MSH-5.1: NMSIIS      MSH-5.2: nmsiis                           MSH-5.3:
MSH-6.1:             MSH-6.2:           MSH-6.3:               Version:
2.5.1
MSH21.1: Z22         MSH21.2: CDCPHINVS
MSH22.1: NMSIIS      MSH22.6:           MSH22.7:       MSH22.10:
MSH23.1:             MSH23.6:           MSH23.7:       MSH23.10:
PID11.7:             RXA-5.1: CVX ONLY                 RXA-6.1 :
File Extension......:                   Protection Indicator: PI NOT NEEDED
Include/Exclude SSN.: EXCLUDE SSN       Include Insurance...: NO
Include/Exclude PV1.: EXCLUDE PV1       Auto Query Mode.....:
Purge Messages after: 90 days           Exchange State......: NEW MEXICO
Barcode/Vac type Seg: VIS BARCODE


     Select one of the following:

          1         Edit parameters for NEW MEXICO
          2         Add specific FACILITY(IES) for NEW MEXICO export
          3         Add NEW MEXICO specific IIS code(s)

Which ADDITIONAL export function for NEW MEXICO: 1  Edit parameters for NEW
MEXI
CO


Additional STATE name........: NEW MEXICO//
Path for OUTBOUND Messages...: g:\smm\nmsiis\request\
           Replace
Path for INBOUND Messages....: g:\smm\nmsiis\response\
           Replace
Ages to Export..............: ALL AGES//
Sending Application   MSH-3.1: nmsiis//
Sending Application   MSH-3.2:
Sending Application   MSH-3.3:
Sending Facility      MSH-4.1: NMSIIS//
Sending Facility      MSH-4.2: nmsiis//
Sending Facility      MSH-4.3:
Receiving Application MSH-5.1: NMSIIS//
Receiving Application MSH-5.2: nmsiis//
Receiving Application MSH-5.3:
Receiving Facility    MSH-6.1:
Receiving Facility    MSH-6.2:
Receiving Facility    MSH-6.3:
Flag TEST messages T  MSH-11.:
HL7 Version in use    MSH-12.: 2.5.1 R1.5 2016+//
Profile Identifier   MSH-21.1: Z22//
Profile Identifier   MSH-21.2: CDCPHINVS//
Responsible Sendng ORG MSH-22: NMSIIS//
Assigning Authority   MSH-22.6:
Idenfifier Type Code  MSH-22.7:
```

```
Sending Org ID      MSH-22.10:
Receiving Org Name    MSH-23.1:
Receiving Org Auth    MSH-23.6:
Receiving Resp Org    MSH-23.7:
Receiving Resp OrgID MSH-23.10:
Primary Facility Name PD1-3.2:
Primary Facility ID-2 PD1-3.3:
CVX or CPT or NDC for RXA-5..: CVX ONLY//
Value for blank volume RXA-6.:
File extension (dat or hl7)..:
Protection Indicator Enforced: PI NOT NEEDED//
Exclude Patient's SSN........: EXCLUDE SSN//
Include Insurance Segments...: NO//
Exclude PV1 Segment..........: EXCLUDE PV1//
Use VIS Barcode or NOS SEGS...:
State site exchanges with....: NEW MEXICO//
```

Figure 3-21: Define Additional Data Exchange Sites option

Appendix A Rules of Behavior

The Resource and Patient Management (RPMS) system is a United States Department of Health and Human Services (HHS), Indian Health Service (IHS) information system that is ***FOR OFFICIAL USE ONLY***. The RPMS system is subject to monitoring; therefore, no expectation of privacy shall be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.

All users (Contractors and IHS Employees) of RPMS will be provided a copy of the Rules of Behavior (ROB) and must acknowledge that they have received and read them prior to being granted access to a RPMS system, in accordance IHS policy.

- For a listing of general ROB for all users, see the most recent edition of *IHS General User Security Handbook* (SOP 06-11a).
- For a listing of system administrators/managers rules, see the most recent edition of the *IHS Technical and Managerial Handbook* (SOP 06-11b).

Both documents are available at this IHS Web site:
https://home.ihs.gov/security/index.cfmhttp://security.ihs.gov/.

> **Note**: Users must be logged on to the IHS D1 Intranet to access these documents.

The ROB listed in the following sections are specific to RPMS.

A.1 All RPMS Users

In addition to these rules, each application may include additional ROBs that may be defined within the documentation of that application (e.g., Dental, Pharmacy).

A.1.1 Access

RPMS users shall

- Only use data for which you have been granted authorization.
- Only give information to personnel who have access authority and have a need to know.
- Always verify a caller's identification and job purpose with your supervisor or the entity provided as employer before providing any type of information system access, sensitive information, or nonpublic agency information.

- Be aware that personal use of information resources is authorized on a limited basis within the provisions *Indian Health Manual* Part 8, "Information Resources Management," Chapter 6, "Limited Personal Use of Information Technology Resources."

RPMS users shall not

- Retrieve information for someone who does not have authority to access the information.
- Access, research, or change any user account, file, directory, table, or record not required to perform their *official* duties.
- Store sensitive files on a PC hard drive, or portable devices or media, if access to the PC or files cannot be physically or technically limited.
- Exceed their authorized access limits in RPMS by changing information or searching databases beyond the responsibilities of their jobs or by divulging information to anyone not authorized to know that information.

A.1.2 Information Accessibility

RPMS shall restrict access to information based on the type and identity of the user. However, regardless of the type of user, access shall be restricted to the minimum level necessary to perform the job.

RPMS users shall

- Access only those documents they created and those other documents to which they have a valid need-to-know and to which they have specifically granted access through an RPMS application based on their menus (job roles), keys, and FileMan access codes. Some users may be afforded additional privileges based on the functions they perform, such as system administrator or application administrator.
- Acquire a written preauthorization in accordance with IHS policies and procedures prior to interconnection to or transferring data from RPMS.

A.1.3 Accountability

RPMS users shall

- Behave in an ethical, technically proficient, informed, and trustworthy manner.
- Log out of the system whenever they leave the vicinity of their personal computers (PCs).
- Be alert to threats and vulnerabilities in the security of the system.
- Report all security incidents to their local Information System Security Officer (ISSO)

- Differentiate tasks and functions to ensure that no one person has sole access to or control over important resources.
- Protect all sensitive data entrusted to them as part of their government employment.
- Abide by all Department and Agency policies and procedures and guidelines related to ethics, conduct, behavior, and information technology (IT) information processes.

A.1.4 Confidentiality

RPMS users shall

- Be aware of the sensitivity of electronic and hard copy information and protect it accordingly.
- Store hard copy reports/storage media containing confidential information in a locked room or cabinet.
- Erase sensitive data on storage media prior to reusing or disposing of the media.
- Protect all RPMS terminals from public viewing at all times.
- Abide by all Health Insurance Portability and Accountability Act (HIPAA) regulations to ensure patient confidentiality.

RPMS users shall not

- Allow confidential information to remain on the PC screen when someone who is not authorized to that data is in the vicinity.
- Store sensitive files on a portable device or media without encrypting.

A.1.5 Integrity

RPMS users shall

- Protect their systems against viruses and similar malicious programs.
- Observe all software license agreements.
- Follow industry standard procedures for maintaining and managing RPMS hardware, operating system software, application software, and/or database software and database tables.
- Comply with all copyright regulations and license agreements associated with RPMS software.

RPMS users shall not

- Violate federal copyright laws.
- Install or use unauthorized software within the system libraries or folders.

- Use freeware, shareware, or public domain software on/with the system without their manager's written permission and without scanning it for viruses first.

A.1.6 System Logon

RPMS users shall

- Have a unique User Identification/Account name and password.
- Be granted access based on authenticating the account name and password entered.
- Be locked out of an account after five successive failed login attempts within a specified time period (e.g., one hour).

A.1.7 Passwords

RPMS users shall

- Change passwords a minimum of every 90 days.
- Create passwords with a minimum of eight characters.
- If the system allows, use a combination of alpha-numeric characters for passwords, with at least one uppercase letter, one lower case letter, and one number. It is recommended, if possible, that a special character also be used in the password.
- Change vendor-supplied passwords immediately.
- Protect passwords by committing them to memory or store them in a safe place (do not store passwords in login scripts or batch files).
- Change passwords immediately if password has been seen, guessed, or otherwise compromised, and report the compromise or suspected compromise to their ISSO.
- Keep user identifications (IDs) and passwords confidential.

RPMS users shall not

- Use common words found in any dictionary as a password.
- Use obvious readable passwords or passwords that incorporate personal data elements (e.g., user's name, date of birth, address, telephone number, or social security number; names of children or spouses; favorite band, sports team, or automobile; or other personal attributes).
- Share passwords/IDs with anyone or accept the use of another's password/ID, even if offered.
- Reuse passwords. A new password must contain no more than five characters per eight characters from the previous password.

- Post passwords.
- Keep a password list in an obvious place, such as under keyboards, in desk drawers, or in any other location where it might be disclosed.
- Give a password out over the phone.

A.1.8 Backups

RPMS users shall

- Plan for contingencies such as physical disasters, loss of processing, and disclosure of information by preparing alternate work strategies and system recovery mechanisms.
- Make backups of systems and files on a regular, defined basis.
- If possible, store backups away from the system in a secure environment.

A.1.9 Reporting

RPMS users shall

- Contact and inform their ISSO that they have identified an IT security incident and begin the reporting process by providing an IT Incident Reporting Form regarding this incident.
- Report security incidents as detailed in the *IHS Incident Handling Guide* (SOP 05-03).

RPMS users shall not

- Assume that someone else has already reported an incident. The risk of an incident going unreported far outweighs the possibility that an incident gets reported more than once.

A.1.10 Session Timeouts

RPMS system implements system-based timeouts that back users out of a prompt after no more than 5 minutes of inactivity.

RPMS users shall

- Utilize a screen saver with password protection set to suspend operations at no greater than 10 minutes of inactivity. This will prevent inappropriate access and viewing of any material displayed on the screen after some period of inactivity.

A.1.11 Hardware

RPMS users shall

- Avoid placing system equipment near obvious environmental hazards (e.g., water pipes).
- Keep an inventory of all system equipment.
- Keep records of maintenance/repairs performed on system equipment.

RPMS users shall not

- Eat or drink near system equipment.

A.1.12 Awareness

RPMS users shall

- Participate in organization-wide security training as required.
- Read and adhere to security information pertaining to system hardware and software.
- Take the annual information security awareness.
- Read all applicable RPMS manuals for the applications used in their jobs.

A.1.13 Remote Access

Each subscriber organization establishes its own policies for determining which employees may work at home or in other remote workplace locations. Any remote work arrangement should include policies that

- Are in writing.
- Provide authentication of the remote user through the use of ID and password or other acceptable technical means.
- Outline the work requirements and the security safeguards and procedures the employee is expected to follow.
- Ensure adequate storage of files, removal, and nonrecovery of temporary files created in processing sensitive data, virus protection, and intrusion detection, and provide physical security for government equipment and sensitive data.
- Establish mechanisms to back up data created and/or stored at alternate work locations.

Remote RPMS users shall

- Remotely access RPMS through a virtual private network (VPN) whenever possible. Use of direct dial in access must be justified and approved in writing and its use secured in accordance with industry best practices or government procedures.

Remote RPMS users shall not

- Disable any encryption established for network, internet, and Web browser communications.

A.2 RPMS Developers

RPMS developers shall

- Always be mindful of protecting the confidentiality, availability, and integrity of RPMS when writing or revising code.
- Always follow the IHS RPMS Programming Standards and Conventions (SAC) when developing for RPMS.
- Only access information or code within the namespaces for which they have been assigned as part of their duties.
- Remember that all RPMS code is the property of the U.S. Government, not the developer.
- Not access live production systems without obtaining appropriate written access and shall only retain that access for the shortest period possible to accomplish the task that requires the access.
- Observe separation of duties policies and procedures to the fullest extent possible.
- Document or comment all changes to any RPMS software at the time the change or update is made. Documentation shall include the programmer's initials, date of change, and reason for the change.
- Use checksums or other integrity mechanism when releasing their certified applications to assure the integrity of the routines within their RPMS applications.
- Follow industry best standards for systems they are assigned to develop or maintain and abide by all Department and Agency policies and procedures.
- Document and implement security processes whenever available.

RPMS developers shall not

- Write any code that adversely impacts RPMS, such as backdoor access, "Easter eggs," time bombs, or any other malicious code or make inappropriate comments within the code, manuals, or help frames.

- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

A.3 Privileged Users

Personnel who have significant access to processes and data in RPMS, such as, system security administrators, systems administrators, and database administrators, have added responsibilities to ensure the secure operation of RPMS.

Privileged RPMS users shall

- Verify that any user requesting access to any RPMS system has completed the appropriate access request forms.
- Ensure that government personnel and contractor personnel understand and comply with license requirements. End users, supervisors, and functional managers are ultimately responsible for this compliance.
- Advise the system owner on matters concerning information technology security.
- Assist the system owner in developing security plans, risk assessments, and supporting documentation for the certification and accreditation process.
- Ensure that any changes to RPMS that affect contingency and disaster recovery plans are conveyed to the person responsible for maintaining continuity of operations plans.
- Ensure that adequate physical and administrative safeguards are operational within their areas of responsibility and that access to information and data is restricted to authorized personnel on a need-to-know basis.
- Verify that users have received appropriate security training before allowing access to RPMS.
- Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs.
- Document and investigate known or suspected security incidents or violations and report them to the ISSO, Chief Information Security Officer (CISO), and systems owner.
- Protect the supervisor, superuser, or system administrator passwords.
- Avoid instances where the same individual has responsibility for several functions (i.e., transaction entry and transaction approval).
- Watch for unscheduled, unusual, and unauthorized programs.
- Help train system users on the appropriate use and security of the system.

- Establish protective controls to ensure the accountability, integrity, confidentiality, and availability of the system.
- Replace passwords when a compromise is suspected. Delete user accounts as quickly as possible from the time that the user is no longer authorized system. Passwords forgotten by their owner should be replaced, not reissued.
- Terminate user accounts when a user transfers or has been terminated. If the user has authority to grant authorizations to others, review these other authorizations. Retrieve any devices used to gain access to the system or equipment. Cancel logon IDs and passwords and delete or reassign related active and backup files.
- Use a suspend program to prevent an unauthorized user from logging on with the current user's ID if the system is left on and unattended.
- Verify the identity of the user when resetting passwords. This can be done either in person or having the user answer a question that can be compared to one in the administrator’s database.
- Shall follow industry best standards for systems they are assigned to and abide by all Department and Agency policies and procedures.

Privileged RPMS users shall not

- Access any files, records, systems, etc., that are not explicitly needed to perform their duties
- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

Glossary

Archiving

The storing of historical or little-used data off-line (often on tape).

Banner

A line of text with a user's name and domain.

Caret (^)

A circumflex, also known as a "hat," used in RPMS to exit from a particular activity or data entry sequence. This special control character is typed by pressing Shift+6 on the keyboard.

Event Type

A message that signifies a particular event on the system (e.g., admit, discharge, etc.).

File

A set of related records or entries treated as a single unit.

HL7

The generally accepted standard for the exchange of certain specified types of medical information between applications. Health Level Seven (HL7) is both the name of the standards developing organization and the collection of protocols that the organization has developed and published. For more information, refer to the HL7 Web site: www.hl7.org.

HL7 Message

An HL7 message consists of a set of message segments that contain the pertinent data for one patient, where each message segment is a group of elements, also known as data fields, which have been defined as logically belonging to the same category, for example, patient immunization.

Menu

A list of choices for computing activity. A menu is a type of option designed to identify a series of items (other options) for presentation to the user for selection. When displayed, menu-type options are preceded by the word "Select" and followed by the word "option" as in Select Menu Management option: (the menu's select prompt).

Option

An entry in the Option file. As an item on a menu, an option provides an opportunity for users to select it, thereby invoking the associated computing activity. Options may also be scheduled to run in the background, noninteractively, by TaskMan

Simple Message Mover (SMM)

SMM is a software program (external to RPMS) that enables a two-way exchange of immunization data between facilities running RPMS and State immunization registries. It uses secured data exchange via HTTPS, to meet HIPAA data security requirements for exchange of information between IHS and Tribal facilities and State registries.

Acronym List

Acronym	Term Meaning
CDC	Centers for Disease Control and Prevention
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level Seven
HTTPS	Hypertext Transfer Protocol Secure
IHS	Indian Health Service
IIMM	Immunization Interface Management Menu
IIS	Immunization Information System
IT	Information Technology
RPMS	Resource and Patient Management System
SIIS	State Immunization Information System
SMM	Simple Message Mover

Contact Information

If you have any questions or comments regarding this distribution, please contact the IHS IT Service Desk.

Phone: (888) 830-7280 (toll free)

Web: https://www.ihs.gov/itsupport/

Email: itsupport@ihs.gov