RESOURCE AND PATIENT MANAGEMENT SYSTEM

Consolidated Clinical Document Architecture (CCDA)

(BCCD)

User Manual

Version 2.0
September 2020

Office of Information Technology
Division of Information Technology

Table of Contents

Trademark Notice

Caché®, Ensemble®, and HealthShare® are registered trademarks of InterSystems Corporation.

Continuity of Care Document® is a registered trademark of Health Level Seven International.

HL7® and Health Level Seven® are registered trademarks of Health Level Seven International.

Windows® is a registered trademark of Microsoft Corporation.

SNOMED® and SNOMED CT® are registered trademarks of the International Health Terminology Standards Development Organization.

UNIX® is a registered trademark of The Open Group.

Preface

This manual provides information for site managers regarding operations of the Consolidated Clinical Document Architecture (CCDA) v2.0 (BCCD) package. This manual is not intended for end users of RPMS since there is no end user functionality in this package.

The BCCD package is designed to generate industry standard Continuity of Care Documents (CCD) in Health Level 7 (HL7) CCDA format, following the August 2015 Draft Standard for Trial Use (DSTU) standard, further restricted by 2015 Certified Health Information Technology (CHIT) requirements. These documents can be transmitted to Indian Health Service (IHS) Health Information Exchange (HIE) repositories, retrieved by the Electronic Health Record (EHR) Graphical User Interface (GUI) using web services, or viewed as export summary documents.

1.0 Introduction

The Consolidated Clinical Document Architecture (CCDA) (namespace BCCD) software is a component of the IHS Resource and Patient Management System (RPMS). The software provides the ability to generate industry standard Clinical Summary, Transitions of Care, Export Summary, Health Information Exchange (HIE) and Case Reporting documents that meet the Health Level Seven (HL7) August 2015 DSTU standard and 2015 CHIT specifications.

Clinical Summary and Transitions of Care documents are retrieved by the EHR GUI using web services. Data Export summary documents are requested via an RPMS Application Programming Interface (API). HIE documents are generated by a nightly background job or via an RPMS menu option and are transmitted to IHS HIE repositories via web services. Case Reporting documents are requested by the iCare (BQI) application, which retrieves completed documents for transmission.

1.1 Purpose

CCDA documents can serve a variety of purposes, including enabling clinician access to patient data in an emergency scenario, quality reporting, bio surveillance, patient access to the patient's own data via a Personal Health Record (PHR) system, and medication or allergy reconciliation.

Each CCDA document consists of two components: a human-readable part known as a narrative block, which can be displayed by a web browser; and a machine-readable part intended for automated data processing. The machine-readable component may contain more detailed information than the human-readable part.

1.2 Scope

A CCDA document is an Extensible Markup Language (XML) document summarizing current and pertinent historical information about an individual patient’s health care record at a given facility. Although not every document type contains every section, the current IHS implementation of the CCDA standard supports the following sections:

- Allergies
- Assessment and Plan
- Care Team
- Case Reporting
- Discharge Diagnoses (inpatient visits only)
- Encounters

- Functional Status
- Goals
- Health Concerns
- Hospital Course (inpatient visits only)
- Hospital Discharge Instructions (displayed for observation [O]and day surgery [S] visits, in addition to inpatient visits)
- Immunizations
- Medical Equipment
- Medications
- Mental Status
- Patient
- Problems/Encounter Diagnoses
- Procedures
- Reason for Hospitalization (inpatient visits only)
- Reason for Referral
- Reason for Visit (ambulatory visits only)
- Results
- Social History (Smoking Status)
- Vital Signs

2.0 System Navigation

2.1 Setup - CCDA

To set up CCDA at an RPMS site:

1. Calculate the additional disk space required for the BCCD application and allocate disk space.
2. Perform pre-install steps, including enabling Long Strings, verifying access to OS configuration file, designating a directory where the new CCDA database will reside, mapping BMW globals, and stopping CCDA.
3. Install the provided Kernel Installation and Distribution System (KIDS) build.
4. Perform post-install steps, including setting up optional encryption, optional e-mail notifications, disabling journaling in the CCDA database, configuring the CCDA CSP Application, setting up site-specific BCCD parameters, and starting CCDA Messaging.

See the *CCDA Installation Manual* for further details on the installation and configuration steps.

The BCCD package has one RPMS menu used by site managers, CCDA MENU (BCCD MENU), which presents the following options:

- Edit CCDA Site Parameters (BCCD EDIT SITE PARAMETERS)
- Edit CCDA Clinical Site Parameters (BCCD EDIT CLINICAL PARAMETERS)
- Generate CCDA for a single patient (BCCD CCDGENONE)
- Generate CCDA documents for all patients in RPMS (BCCD CCDALLGEN)
- Generate CCDA documents for a specified date range (BCCD GEN CCDA DATE RANGE)
- Manage CCDA transmissions (BCCD CCDA MGR)
- View and Purge Error Documents (BCCD ERROR PURGE)
- Display the CCDA application status report (BCCD APP STATUS)

The BCCD package contains no menu options accessible by end users.

Site managers are responsible for performing the following two tasks to ensure that CCDA documents are successfully generated at their site:

1. Ensure that site-specific CCDA parameters are set up appropriately. Section 3.1 provides more information about the set up.

2. Ensure that CCDA Messaging is running. Section 3.2 provides more information about managing CCDA Messaging.

2.2 Setup - Hospital Course Information

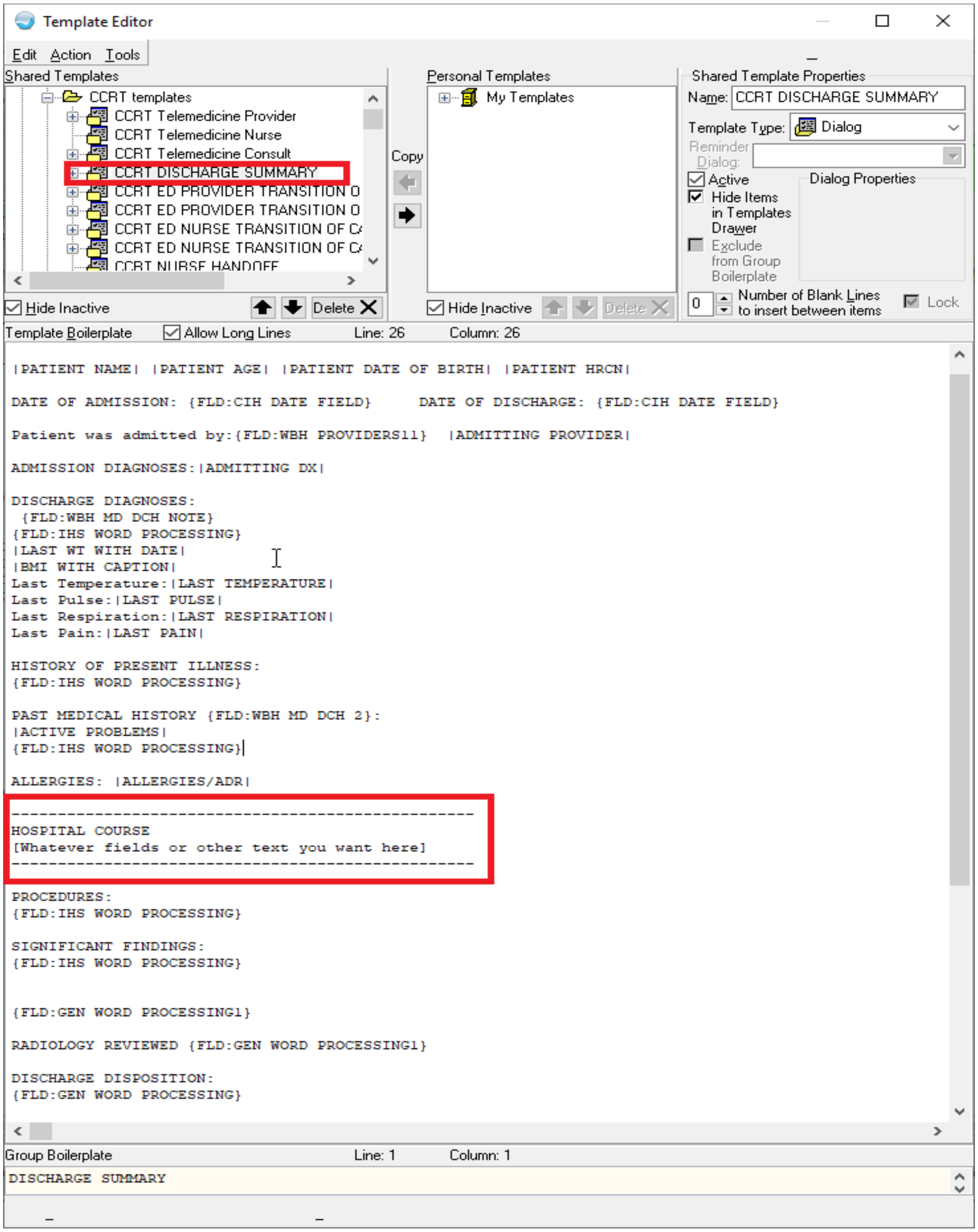
BCCD v2.0 added a new section to inpatient CCDA documents called Hospital Course. The information for the Hospital Course section comes from the Discharge Summary TIU note associated with the Inpatient stay.

> **Note:** The Discharge Summary note may include additional information not related to the Hospital Course.

To extract only the Hospital Course information only in the CCDA from the Discharge Summary note, it is recommended that any Discharge Summary template have a Hospital Course header and footer. The header should be 50 hyphens on their own line followed by the text "HOSPITAL COURSE" (without quotes) on its own line. The footer should follow the Hospital Course information and be 50 hyphens on its own line.

Later, when the provider creates the Discharge Summary note for the patient, the Hospital Course information must be entered by the provider between the header and footer; otherwise the CCDA will include all the information entered in the Discharge Summary note. To make it easier for the provider to identify what is the header and footer, you may want to consider entering some blank lines between the header and footer.

> **Note:** Please work with your Clinical Informaticists on entering the Hospital Course header and footer. An example of how to add the Hospital Course header and footer to a Discharge Summary template is shown in the Figure 2-1.



Name: CCRT DISCHARGE SUMMARY

Template Type: Dialog

Reminder Dialog:

☑ Active

☑ Hide Items in Templates Drawer

☐ Exclude from Group Boilerplate

0 Number of Blank Lines to insert between items

☑ Lock

☑ Hide Inactive

☑ Allow Long Lines Line: 26 Column: 26

```
|PATIENT NAME| |PATIENT AGE| |PATIENT DATE OF BIRTH| |PATIENT HRCN|

DATE OF ADMISSION: {FLD:CIH DATE FIELD}     DATE OF DISCHARGE: {FLD:CIH DATE FIELD}

Patient was admitted by:{FLD:WBH PROVIDERS11}  |ADMITTING PROVIDER|

ADMISSION DIAGNOSES:|ADMITTING DX|

DISCHARGE DIAGNOSES:
 {FLD:WBH MD DCH NOTE}
{FLD:IHS WORD PROCESSING}
|LAST WT WITH DATE|
|BMI WITH CAPTION|
Last Temperature:|LAST TEMPERATURE|
Last Pulse:|LAST PULSE|
Last Respiration:|LAST RESPIRATION|
Last Pain:|LAST PAIN|

HISTORY OF PRESENT ILLNESS:
{FLD:IHS WORD PROCESSING}

PAST MEDICAL HISTORY {FLD:WBH MD DCH 2}:
|ACTIVE PROBLEMS|
{FLD:IHS WORD PROCESSING}

ALLERGIES: |ALLERGIES/ADR|

--------------------------------------------------
HOSPITAL COURSE
[Whatever fields or other text you want here]
--------------------------------------------------
PROCEDURES:
{FLD:IHS WORD PROCESSING}

SIGNIFICANT FINDINGS:
{FLD:IHS WORD PROCESSING}


{FLD:GEN WORD PROCESSING1}

RADIOLOGY REVIEWED {FLD:GEN WORD PROCESSING1}

DISCHARGE DISPOSITION:
{FLD:GEN WORD PROCESSING}
```

Group Boilerplate Line: 1 Column: 1

```
DISCHARGE SUMMARY
```

Figure 2-1: Adding Hospital Course Header and Footer to a Discharge Summary template

2.3 Architecture

CCDA processing can be initiated in four ways:

- If EHR version 1.1, patch 13 has been installed and configured at the site, then authorized EHR users are able to request Clinical Summary and Transitions of Care documents for display within the EHR GUI client.
- If the site is a part of the IHS HIE, then HIE documents are generated nightly for all patients whose data has changed since the previous nightly upload.
- Data Export summary documents can be generated for specific patients or for all patients via an RPMS API.
- Case Reporting documents are requested by the iCare (BQI) application, which retrieves completed documents for transmission.

To accommodate requests from the EHR GUI, Ensemble has a web service process listening for requests for Clinical Summary and Transitions of Care documents.

If the site is part of the IHS HIE, a nightly TaskMan task called BCCD NHIE PUSH JOB is automatically scheduled to run every night at the time specified by the site manager in option Edit CCDA Site Parameters. When BCCD NHIE PUSH JOB runs for the first time, it creates new CCDA requests for all patients in the RPMS database. On subsequent executions, BCCD NHIE PUSH JOB finds all patients whose data has changed since the last time it ran and creates new requests in the CCDA queue.

To request Data Export summary documents, the site manager accesses an RPMS API. In order to prevent unintended initiation of Data Export documents, the API is not included as an RPMS option in the menu system. Instead, the site manager must first access Programmer Mode, then enter the necessary command. Because it is expected that this Data Export functionality will rarely, if ever, be used, the IHS Software Quality Assurance (SQA) team will distribute instructions for generating Data Export documents on an “as needed” basis.

Case Reporting documents are requested and processed by the iCare (BQI) application. Details on this process are outside the scope of this document. For further information, consult the appropriate iCare documentation.

The only difference between CCDA requests created by these four mechanisms is that the DocType property is set to the requested document type and several flags are set to control where the documents are sent. For all CCDA requests, a new entry is placed in the CCDA queue, recording the IDs of the requested patient and visit(s), and sets the record’s status to R (for Request).

The CCDA queue is monitored by BCCD BACKGROUND JOB, the main CCDA generator. The BCCD BACKGROUND JOB is a persistent TaskMan job started at TaskMan startup time, or manually from menu option Manage CCDA transmissions which constantly runs in the background until the site manager chooses to stop CCDA. When the BCCD BACKGROUND JOB finds a new CCDA request with the status of R in the CCDA queue, it changes the request's status to CS (for Compile Started) and extracts all relevant RPMS data for the specified patient and visit and adds the data to the body of the CCDA request. Depending on the amount of eligible data in the patient's records, it may take anywhere from under a second to over 10 seconds to extract all needed data from RPMS.

Once the extraction process for the patient is finished, BCCD BACKGROUND JOB changes the status of the request to CE (for Compile Ended). The BCCD BACKGROUND JOB then checks the CCDA queue for other outstanding requests with the status of R. If no outstanding requests are found, the BCCD BACKGROUND JOB goes into hibernation for a specific amount of time, usually one second.

The CCDA queue is also monitored by the CCDA Ensemble production running in the CCDA namespace. When the CCDA production finds a new request, whose status is set to CE, it retrieves the CCDA data from the body of the request, changes the status to TS (for Transmission Started), and transforms it into a valid CCDA document. For EHR Clinical Summary and Transitions of Care requests, the document is sent back to the requesting EHR. For Data Export and Case Reporting, the production saves this document to a file. For HIE documents, the production transmits it to an IHS HIE. Finally, the production changes the status of the request to T (for Transmitted).

If a site is a part of the IHS HIE, then the site manager is provided with the URL of the associated CCDA repository. Ensemble uses this URL to send CCDA documents to the repository. HIE CCDA processing typically occurs at night to minimize the impact on RPMS performance.

3.0 Package Management

3.1 Manage Site-Specific CCDA Parameters

The RPMS option **Edit CCDA Site Parameters (BCCD EDIT SITE PARAMETERS)** has been divided into two options with different security keys.

3.1.1 Edit CCDA Site Parameters

The option **Edit CCDA Site Parameters (BCCD EDIT SITE PARAMETERS)** allows site managers to configure site-specific CCDA parameters at installation time and modify them if necessary.

> **Note:** This menu option is locked by security key XUMGR, which site managers already have.

The following four parameters can be edited using this option:

- TIME TO RUN NIGHTLY TASK
- DAYS KEEP TRANSMISSION ENTRIES
- REPOSITORY LOCATION
- ENABLED

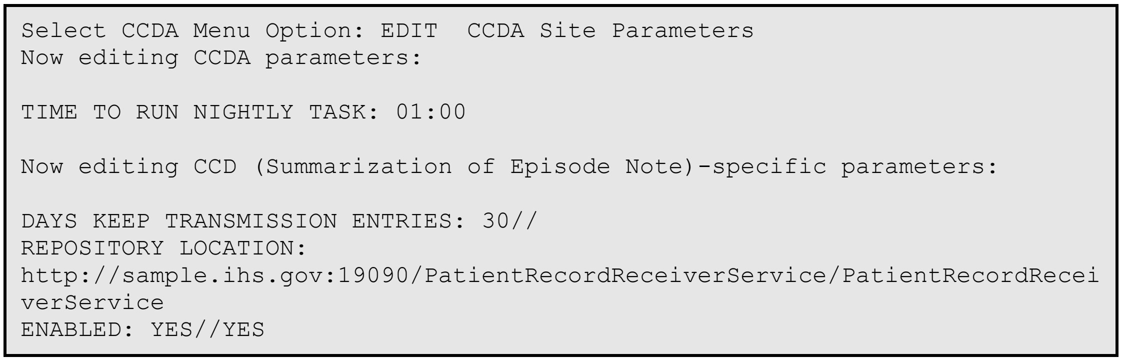
The first prompt is “TIME TO RUN NIGHTLY TASK” and there is no default value. If the RPMS site is not a part of the IHS HIE at this time, then skip the “TIME TO RUN NIGHTLY TASK” prompt. If the RPMS site is a part of the IHS HIE and the site manager has been provided with the location of the off-site CCDA repository, then enter the time when the site wants CCDA documents to be generated and transmitted on a nightly basis. It is recommended to enter a time outside of the regular business hours to minimize impact on the end users. The “TIME TO RUN NIGHTLY TASK “prompt accepts time values in all valid FileMan formats, e.g., 15:34 or 03:34PM.

The second prompt is “DAYS KEEP TRANSMISSION ENTRIES” and it is set to 30 days by default. The value may be set to any value between 7 and 999 days. The higher the number, the more disk space the intermediate compile structures created by the CCDA application will consume as described in Section 3.3 of this installation guide. On the other hand, if the default value is set too low, the compile data may be purged too soon and will not be available to facilitate debugging should any problems arise. If the site manager is not sure what value to enter, accept the default value of 30 days.

The third prompt is “REPOSITORY LOCATION” and there is no default value. If the RPMS site is not a part of the IHS HIE at this time, then skip the “REPOSITORY LOCATION” prompt. If the RPMS site is a part of the IHS HIE and the site manager has been provided with the location of the off-site CCDA repository, then enter that location at the “REPOSITORY LOCATION” prompt exactly as it was provided to the site manager. When a value is entered for both the “REPOSITORY LOCATION” and the “TIME TO RUN NIGHTLY TASK” prompts, the system will check whether the CCDA database has enough disk space to accommodate the process of generating CCDA documents for all patients in the system. An error message will be displayed if there is not enough disk space. If not enough disk space error message displays, allocate more disk space and try again.

The fourth prompt is “ENABLED”, and the default value is **NO**. This **NO** value controls whether CCDA documents are generated when CCDA is running. Change this value to **YES**.

Figure 3-1 contains a screen capture of a typical setup session.



```
Select CCDA Menu Option: EDIT  CCDA Site Parameters
Now editing CCDA parameters:

TIME TO RUN NIGHTLY TASK: 01:00

Now editing CCD (Summarization of Episode Note)-specific parameters:

DAYS KEEP TRANSMISSION ENTRIES: 30//
REPOSITORY LOCATION:
http://sample.ihs.gov:19090/PatientRecordReceiverService/PatientRecordRecei
verService
ENABLED: YES//YES
```

Figure 3-1: Setting up CCDA Site Parameters

3.1.2 Edit CCDA Clinical Site Parameters

The option **Edit CCDA Clinical Site Parameters (BCCD EDIT CLINICAL PARAMETERS)** allows clinicians to configure site-specific clinical CCDA parameters at installation time and modify them if necessary.

> **Note:** This menu option is locked by security key BCCDZCLIN, which must be assigned before the option can be used.

The following four parameters can be edited using this option:

- ADD SOCIAL ENVIRONMENT PROB
- ADD INACTIVE PERS HISTORY PROB
- DISCHARGE PLANNER PROV TYPE

- DISPLAY THE LAST SMOKING STATUS START/END DATE (S), THE LAST MODIFIED DATE (L) OR NO DATE (N)

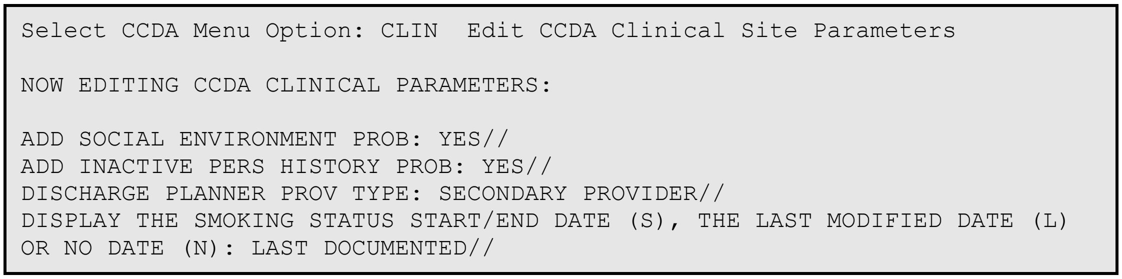
The first prompt is “ADD SOCIAL ENVIRONMENT PROB”, which is set to **NO** by default. This **NO** value determines whether social environment problems will be included in Clinical Summary documents for the site. All other document types will always display the social environment problems.

The second prompt is “ADD INACTIVE PERS HISTORY PROB”, which is set to **NO** by default. This **NO** value specifies whether inactive personal problems are included in Clinical Summary documents for site. All other document types will always display the inactive personal history problem.

The third prompt is “DISCHARGE PLANNER PROV TYPE”, which has no default value. This parameter specifies the BDP DESG SPECIALTY PROVIDER type to be extracted and displayed as the discharge planner on an inpatient CCDA document.

The fourth prompt is “DISPLAY THE SMOKING STATUS START/END DATE (S), THE LAST MODIFIED DATE (L) OR NO DATE (N)” parameter, which is set to L (LAST MODIFIED DATE) by default. If it is set to L (LAST MODIFIED DATE), then the Social History section of the document will display the smoking status date with the label “Last Documented Date”. If it is set to **S (START/END DATE)**, then the Social History section of the document will display the smoking status date with the label “Start Date”. If it is set to **N (NO DATE)**, the smoking status date will not be displayed in the Social History section.

Figure 3-2 contains a screen capture of a typical setup session.



```
Select CCDA Menu Option: CLIN  Edit CCDA Clinical Site Parameters

NOW EDITING CCDA CLINICAL PARAMETERS:

ADD SOCIAL ENVIRONMENT PROB: YES//
ADD INACTIVE PERS HISTORY PROB: YES//
DISCHARGE PLANNER PROV TYPE: SECONDARY PROVIDER//
DISPLAY THE SMOKING STATUS START/END DATE (S), THE LAST MODIFIED DATE (L)
OR NO DATE (N): LAST DOCUMENTED//
```

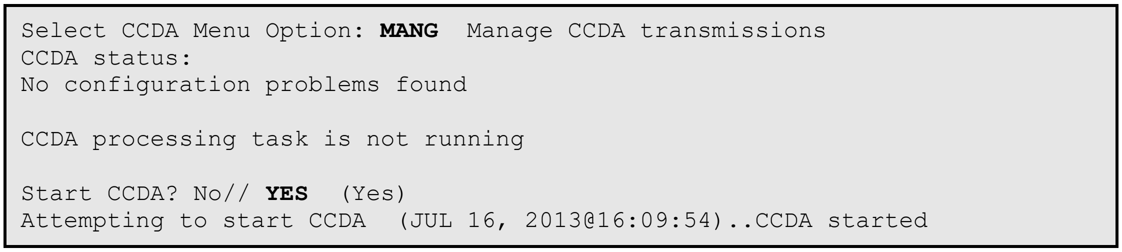
Figure 3-2: Setting up CCDA Clinical Site Parameters

3.2 Manage CCDA Messaging

CCDA Messaging is automatically started whenever TaskMan starts, which typically occurs when Ensemble is started. CCDA Messaging will not run if TaskMan is not running.

CCDA Messaging should be running at all times and does not require a manual start or stop once it has been installed. However, if the need arises, CCDA Messaging can be brought up or down using the **Manage CCDA transmissions** option, which is available in the CCDA Menu. The CCDA Menu can be accessed from the regular "OPTION NAME" prompt in RPMS.

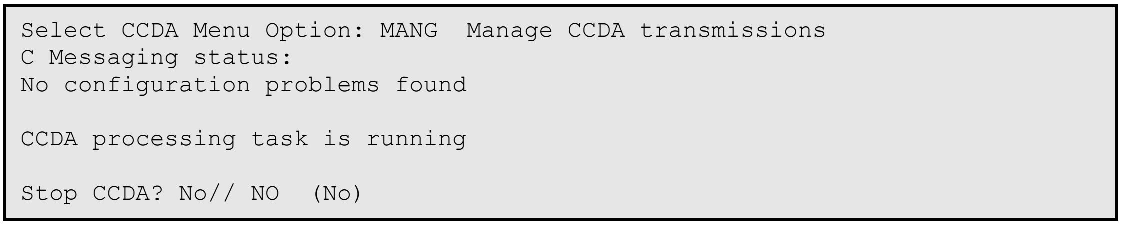
If CCDA Messaging is not running, type **YES** at the prompt as shown in Figure 3-3:



```
Select CCDA Menu Option: MANG  Manage CCDA transmissions
CCDA status:
No configuration problems found

CCDA processing task is not running

Start CCDA? No// YES  (Yes)
Attempting to start CCDA  (JUL 16, 2013@16:09:54)..CCDA started
```

Figure 3-3: Starting CCDA Messaging

If CCDA Messaging is running, type **NO** at the prompt as shown in Figure 3-4:



```
Select CCDA Menu Option: MANG  Manage CCDA transmissions
C Messaging status:
No configuration problems found

CCDA processing task is running

Stop CCDA? No// NO  (No)
```

Figure 3-4: CCDA Messaging already running

3.3 Manage CCDA Ensemble Production

As described in Section 2.2, if the RPMS site is a part of the IHS HIE, CCDA documents are sent to outside repositories using the CCDA Ensemble production. In addition, if EHR version 1.1, patch 13 is installed and configured, authorized EHR users can send requests for CCDA documents to the CCDA Ensemble production.

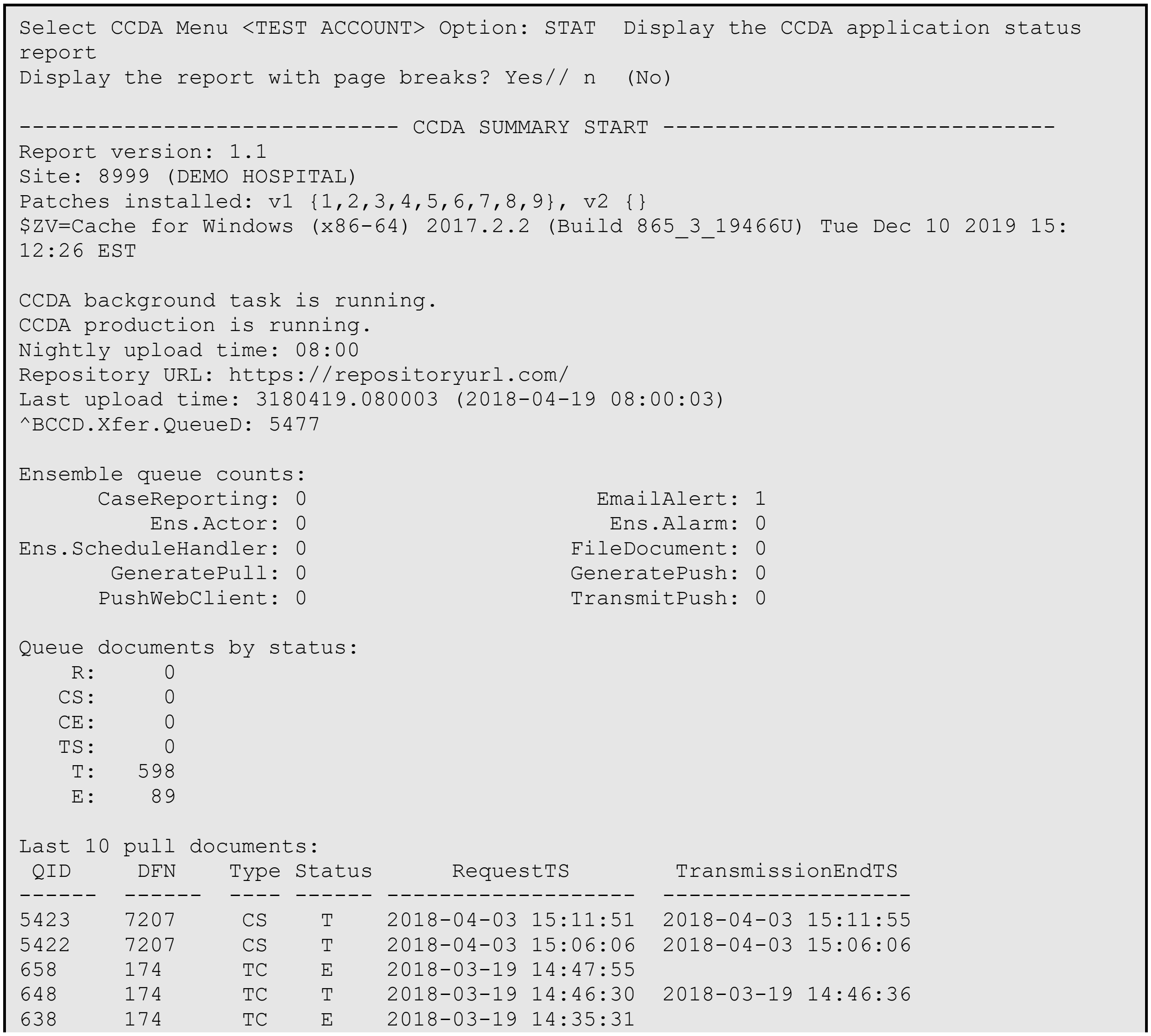
The CCDA Ensemble production is automatically started when HealthShare starts up. During normal business operations, the CCDA Ensemble production will remain running and will not require maintenance. Refer to the Managing CCDA Ensemble Production section in the *CCDA Technical Manual* to bring the CCDA Ensemble production up or down manually, if required.

3.4 CCDA Application Status Report

The **STAT (Display the CCDA application status report)** option may be used to display a report summarizing various information about the state of the CCDA application, as well as information about the most recent pull, push, and error messages. The intent of the report is to provide support personnel with a snapshot of the application. It is not intended to be used by site managers, and no information is provided to assist site managers with interpreting the report.

When the user runs the report, it will ask whether to display the report with page breaks. If the user intends to view the report on the screen, it is recommended that page breaks be used. If the user is running the report in order to copy and paste information for the support team, then not using page breaks may be preferred.

A sample report is shown in Figure 3-5:



```
Select CCDA Menu <TEST ACCOUNT> Option: STAT  Display the CCDA application status
report
Display the report with page breaks? Yes// n  (No)

----------------------------- CCDA SUMMARY START ------------------------------
Report version: 1.1
Site: 8999 (DEMO HOSPITAL)
Patches installed: v1 {1,2,3,4,5,6,7,8,9}, v2 {}
$ZV=Cache for Windows (x86-64) 2017.2.2 (Build 865_3_19466U) Tue Dec 10 2019 15:
12:26 EST

CCDA background task is running.
CCDA production is running.
Nightly upload time: 08:00
Repository URL: https://repositoryurl.com/
Last upload time: 3180419.080003 (2018-04-19 08:00:03)
^BCCD.Xfer.QueueD: 5477

Ensemble queue counts:
      CaseReporting: 0                      EmailAlert: 1
          Ens.Actor: 0                       Ens.Alarm: 0
Ens.ScheduleHandler: 0                    FileDocument: 0
       GeneratePull: 0                    GeneratePush: 0
      PushWebClient: 0                    TransmitPush: 0

Queue documents by status:
    R:     0
   CS:     0
   CE:     0
   TS:     0
    T:   598
    E:    89

Last 10 pull documents:
 QID     DFN    Type Status      RequestTS        TransmissionEndTS
------  ------  ---- ------ -------------------  -------------------
5423    7207     CS    T    2018-04-03 15:11:51  2018-04-03 15:11:55
5422    7207     CS    T    2018-04-03 15:06:06  2018-04-03 15:06:06
658     174      TC    E    2018-03-19 14:47:55
648     174      TC    T    2018-03-19 14:46:30  2018-03-19 14:46:36
638     174      TC    E    2018-03-19 14:35:31
```

```
628     174      TC    T    2018-03-19 14:34:22  2018-03-19 14:34:36
608     4000     TC    T    2018-03-19 14:33:33  2018-03-19 14:33:35
588     4000     TC    T    2018-03-19 14:32:25  2018-03-19 14:32:26
583     4000     TC    T    2018-03-19 14:31:55  2018-03-19 14:31:56
579     4000     TC    T    2018-03-19 14:31:32  2018-03-19 14:31:34

Last 10 push documents:
 QID     DFN    Type Status      RequestTS        TransmissionEndTS
------  ------  ---- ------ -------------------  -------------------
5477    7207     HIE   T    2018-04-19 12:34:45
5476    7207     HIE   T    2018-04-19 12:30:57
5475    7207     HIE   T    2018-04-19 11:40:00
5474    7207     HIE   T    2018-04-19 08:03:38
5473    7207     HIE   T    2018-04-18 19:23:26
5467    1937     HIE   T    2018-04-18 08:01:38
5468    2195     HIE   T    2018-04-18 08:01:38
5469    4432     HIE   T    2018-04-18 08:01:38
5470    4432     HIE   T    2018-04-18 08:01:38
5471    5651     HIE   T    2018-04-18 08:01:38

Last 5 error documents:
 QID    Type      RequestTS                ErrorText
------  ---- ------------------- ------------------------------------------
5476    HIE  2018-04-19 12:30:57 Transmission error: ERROR #6241: The SOAP WebCl
ient LOCATION parameter must specify http or https transport.

5475    HIE  2018-04-19 11:40:00 Transmission error: ERROR #6241: The SOAP WebCl
ient LOCATION parameter must specify http or https transport.

5474    HIE  2018-04-19 08:03:38 Transmission error: ERROR #6241: The SOAP WebCl
ient LOCATION parameter must specify http or https transport.

5463    HIE  2018-04-12 08:01:42 Transmission error: ERROR #6241: The SOAP WebCl
ient LOCATION parameter must specify http or https transport.

5464    HIE  2018-04-12 08:01:42 Transmission error: ERROR #6241: The SOAP WebCl
ient LOCATION parameter must specify http or https transport.
------------------------------ CCDA SUMMARY END --------------------------------
```

Figure 3-5: Sample CCDA application status report

Due to different rules surrounding patient DFNs, some sites may want to prevent DFNs from displaying on the report. To suppress DFNs site-wide, go to RPMS programmer mode and run the following command:

```
DO DFNOFF^BCCDSTAT
```

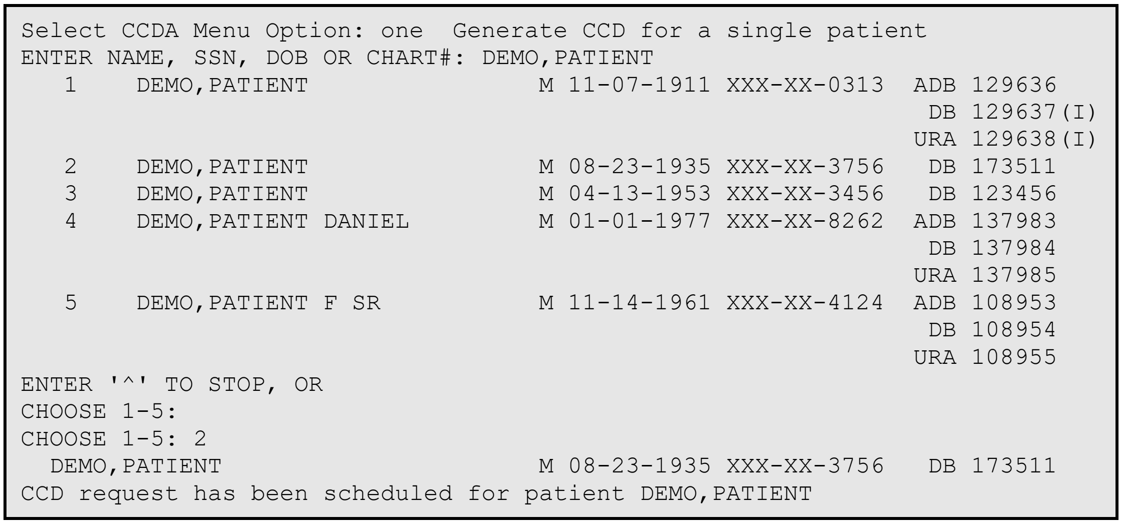
To clear the setting and re-enable DFNs on the report, go to RPMS programmer mode and run the following command:

```
DO DFNCLR^BCCDSTAT
```

4.0 Package Operation

4.1 Manually Generate One CCDA Document

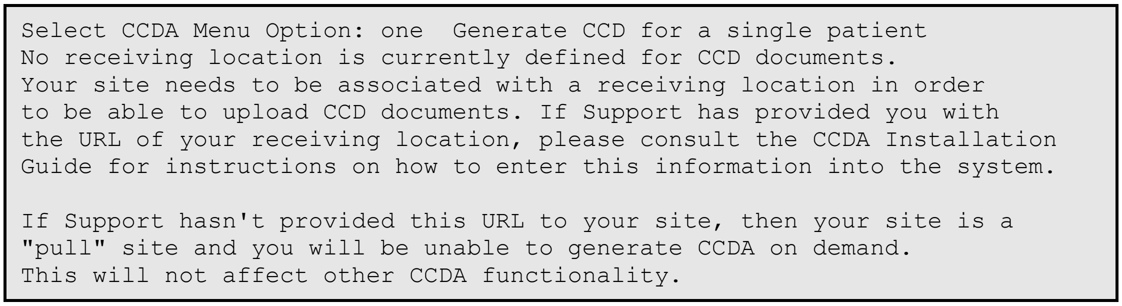
CCDA documents are generated automatically and the process does not require manual intervention. However, on occasion, the site manager may be asked to regenerate the CCDA document for one or more patients. Select the **Generate CCD for a single patient (BCCD CCDGENONE)** option in the **CCDA Menu (BCCD Menu)**. Enter the patient by name, Social Security Number (SSN), date of birth, or chart number. If multiple patients match the input criteria, select the correct patient from the list displayed as shown in Figure 4-1:



```
Select CCDA Menu Option: one  Generate CCD for a single patient
ENTER NAME, SSN, DOB OR CHART#: DEMO,PATIENT
   1    DEMO,PATIENT                M 11-07-1911 XXX-XX-0313  ADB 129636
                                                               DB 129637(I)
                                                              URA 129638(I)
   2    DEMO,PATIENT                M 08-23-1935 XXX-XX-3756   DB 173511
   3    DEMO,PATIENT                M 04-13-1953 XXX-XX-3456   DB 123456
   4    DEMO,PATIENT DANIEL         M 01-01-1977 XXX-XX-8262  ADB 137983
                                                               DB 137984
                                                              URA 137985
   5    DEMO,PATIENT F SR           M 11-14-1961 XXX-XX-4124  ADB 108953
                                                               DB 108954
                                                              URA 108955
ENTER '^' TO STOP, OR
CHOOSE 1-5:
CHOOSE 1-5: 2
  DEMO,PATIENT                      M 08-23-1935 XXX-XX-3756   DB 173511
CCD request has been scheduled for patient DEMO,PATIENT
```

Figure 4-1: Manually regenerating the CCDA document for one patient

> **Note:** The **Generate CCD for a single patient** option only works if the RPMS site is a part of the IHS HIE. Accessing this option at a site that is not a part of the IHS HIE will generate the error message shown in Figure 4-2:

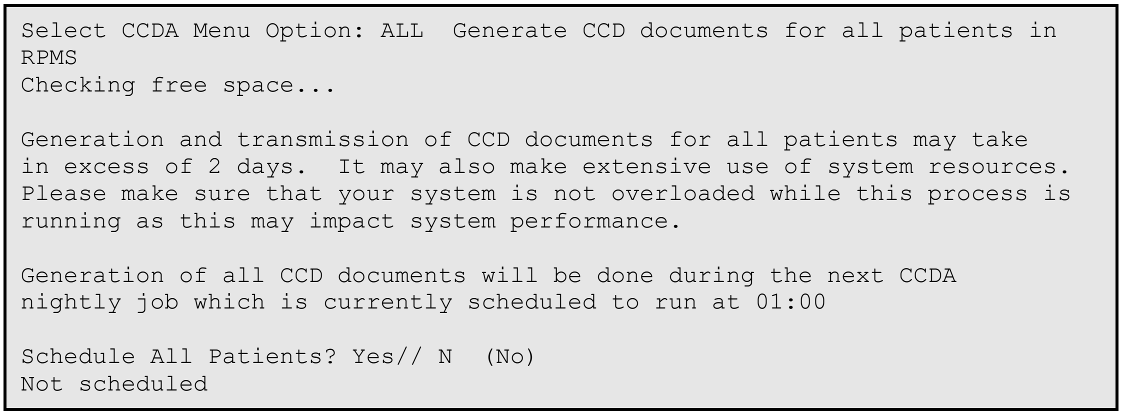


```
Select CCDA Menu Option: one  Generate CCD for a single patient
No receiving location is currently defined for CCD documents.
Your site needs to be associated with a receiving location in order
to be able to upload CCD documents. If Support has provided you with
the URL of your receiving location, please consult the CCDA Installation
Guide for instructions on how to enter this information into the system.

If Support hasn't provided this URL to your site, then your site is a
"pull" site and you will be unable to generate CCDA on demand.
This will not affect other CCDA functionality.
```

Figure 4-2: Error message when trying to manually regenerate a CCDA document at a site that is not a part of the IHS HIE

4.2 Manually Regenerate All CCDA Documents

If the RPMS site is a part of the IHS HIE, then, on rare occasions, the Help Desk may ask the Site Manager to regenerate CCDA documents for all patients in the database. When this happens, select the **Generate CCD documents for all patients in RPMS (BCCD CCDALLGEN)** option in the **CCDA Menu (BCCD Menu)**. The system will check if there is enough disk space for this process and display the warning shown in Figure 4-3:

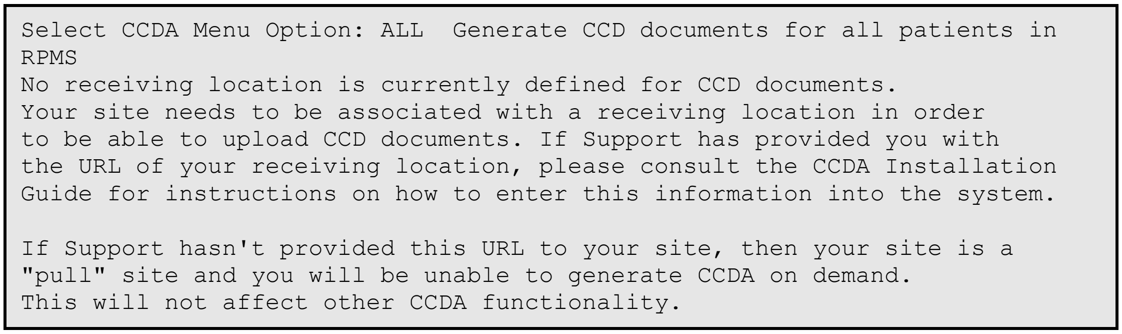


```
Select CCDA Menu Option: ALL  Generate CCD documents for all patients in
RPMS
Checking free space...

Generation and transmission of CCD documents for all patients may take
in excess of 2 days.  It may also make extensive use of system resources.
Please make sure that your system is not overloaded while this process is
running as this may impact system performance.

Generation of all CCD documents will be done during the next CCDA
nightly job which is currently scheduled to run at 01:00

Schedule All Patients? Yes// N  (No)
Not scheduled
```

Figure 4-3: Manually Regenerating All CCDA Documents

Enter **Y** (Yes) or **N** (No) to confirm regeneration of CCDA documents for all patients.

Accessing this option at a site that is not a part of the IHS HIE will generate the error message shown in Figure 4-4:

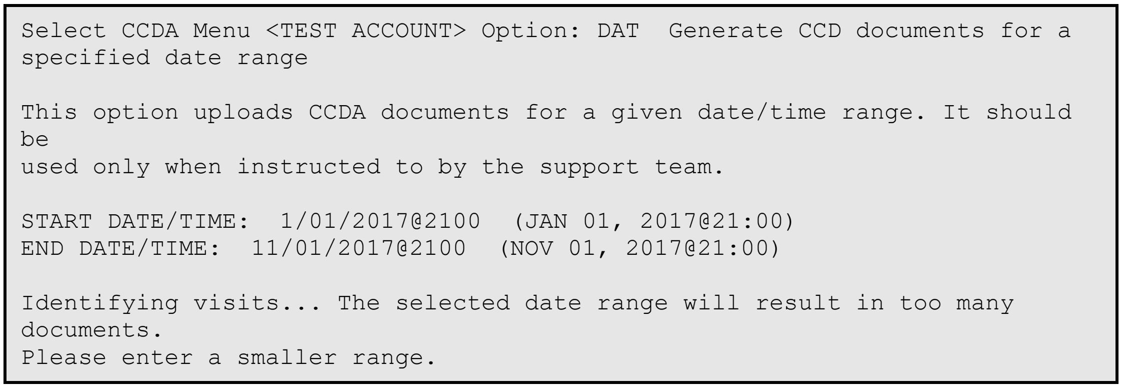


```
Select CCDA Menu Option: ALL  Generate CCD documents for all patients in
RPMS
No receiving location is currently defined for CCD documents.
Your site needs to be associated with a receiving location in order
to be able to upload CCD documents. If Support has provided you with
the URL of your receiving location, please consult the CCDA Installation
Guide for instructions on how to enter this information into the system.

If Support hasn't provided this URL to your site, then your site is a
"pull" site and you will be unable to generate CCDA on demand.
This will not affect other CCDA functionality.
```

Figure 4-4: Error message when trying to manually regenerate all CCDA documents at a site that is not a part of the IHS HIE

4.3 Manually Regenerate CCDA Documents for a Specified Date Range

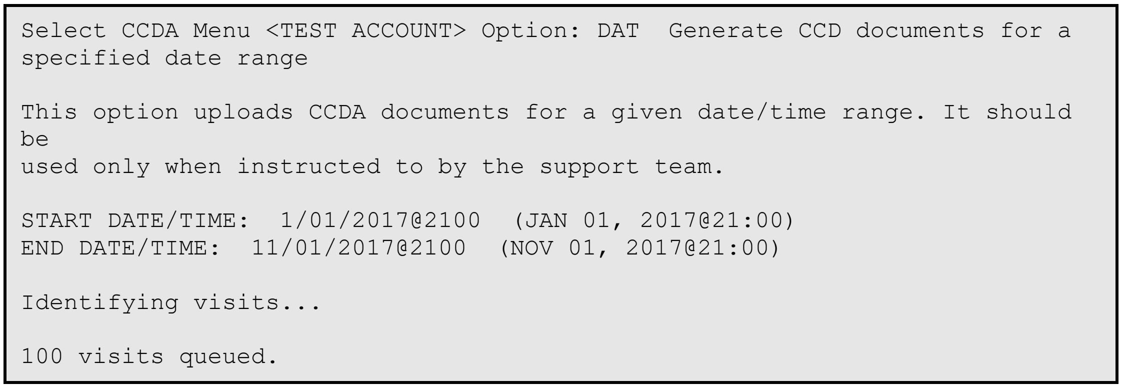
If the RPMS site is a part of the IHS HIE, then, on rare occasions, the Help Desk may ask the Site Manager to regenerate CCDA documents for all visits updated in a specified date range. When this happens, select the **Generate CCD documents for a specified date range (BCCD GEN CCD DATE RANGE)** option in the **CCDA Menu (BCCD Menu)**. The application will ask the user for the start date/time and end date/time for the range. The application will then check whether the date range will result in an excessive number of documents generated. If the number of documents would exceed the maximum number allowed, the system will display the message shown in Figure 4-5:



```
Select CCDA Menu <TEST ACCOUNT> Option: DAT  Generate CCD documents for a
specified date range

This option uploads CCDA documents for a given date/time range. It should
be
used only when instructed to by the support team.

START DATE/TIME:  1/01/2017@2100  (JAN 01, 2017@21:00)
END DATE/TIME:  11/01/2017@2100  (NOV 01, 2017@21:00)

Identifying visits... The selected date range will result in too many
documents.
Please enter a smaller range.
```

Figure 4-5: Generate CCD documents for a specified date range option when selected range is too big

If the number of documents is within the allowed limit, the system will queue the document requests and display the message shown in Figure 4-6:



```
Select CCDA Menu <TEST ACCOUNT> Option: DAT  Generate CCD documents for a
specified date range

This option uploads CCDA documents for a given date/time range. It should
be
used only when instructed to by the support team.

START DATE/TIME:  1/01/2017@2100  (JAN 01, 2017@21:00)
END DATE/TIME:  11/01/2017@2100  (NOV 01, 2017@21:00)

Identifying visits...

100 visits queued.
```

Figure 4-6: Generate CCD documents for a specified date range option when selected range is sufficiently small

5.0 CCDA Audit Log

The CCDA application contains the global ^BCCD.Audit.AuditLogD, which is used to store the CCDA audit log. The CCDA Audit Log table contains audit information about specific requests for CCDA data that come from the EHR GUI, nightly uploads to the HIE, and for documents generated for Data Export. Prior to Patch 6 of Version 1, the audit log was stored in the CCDA database. Patch 6 of Version 1moved the audit log to the RPMS database to make it easier for sites to journal and back up the audit log.

Please refer to the AU - Audit and Accountability section in the *CCDA Security Manual* for instructions to view the data stored in the CCDA Audit Log.

6.0 Limits on the Data Included in CCDA Documents

CCDA documents should contain "current and relevant historical" summary information about patients, which means only recent clinical data is extracted from RPMS and included in CCDA documents except as noted below.

The five types of CCDA documents are:

- Clinical Summary (CS)
- Transitions of Care (ToC)
- Data Export Summary (DP)
- Health Information Exchange Document (HIE)
- Case Reporting (CR) – Sent to Division of Epidemiology

Table 6-1 describes the time ranges and data limitations used to extract RPMS data for individual CCDA modules.

Table 6-1: CCDA Data Limitations

CCDA Module	CCDA Document	Data Extract
Allergies	All	• Extract all Allergies (active and inactive) for the patient.

CCDA Module	CCDA Document	Data Extract
Assessment and Plan	All	• For each Problem that is POV for the encounter, extract: ◦ The Care Plan ◦ The Visit Instructions ◦ The Treatment/Regimen ◦ The Request/Consultations ◦ The Ordered/Pending Lab Tests, ◦ The Lab Tests Awaiting Results • In addition, extract all the below whether associated with a problem or not: ◦ Ordered/Pending Lab and Radiology Tests ◦ All Lab/Radiology Tests awaiting Results ◦ All Referrals ◦ All Requests/Consultations ◦ All Future Appointments • Finally, extract all Treatment/Regimen not associated with a problem
Care Team	All	• Extract the Visit Provider, Attending and Admitting providers (Inpatient), and Referring Providers associated with the visit. • Extract all Specialty Providers associated with the patient.
Discharge Diagnoses	All (Inpatient only)	• For inpatient only, extract the primary of Purpose of Visit
Encounters	All	• Extract the visit for which the document is being created • Extract all Hospitalization, Observation, Nursing Home, Same Day Surgery encounters going back one year from the date of the visit for which the document is being created. • Extract all Ambulatory and TeleMedicine encounters that are workload reportable going back one year going back one year from the date of the visit for which the document is being created. • For each encounter, extract the Purpose of Visit for the encounter.

CCDA Module	CCDA Document	Data Extract
Functional Status	CS	• Not extracted.
Functional Status	ToC, DP, HIE, CR	• Fall Risk: Extract the most recent Fall Risk entry for the patient from the Examinations file • Elder Care Questions: Extract the most recent entry for the patient. • Problems: Extract the subset of SNOMED codes determined to be related to functional status (EHR IPL FUNCTIONAL STATUS).
General Header	All	• Visit Date and Location are visit-specific.
Goals	All	• Extract all Patient Goals that have a status of Active or Maintaining Goal. • Extract all active or met Care Plan goals that are associated with the visit.
Health Concerns	All	• Extract Chronic, Episodic, Environmental/Social History, Personal History/Inactive, and Sub-acute problems. • Extract any problems used as POV for that Encounter (mark with an asterisk). • Extract any POVs for that Encounter (mark with an asterisk). • Extract all Patient Goals that have a status of Active or Maintaining Goal
Hospital Course	All (Inpatient only)	• Extract the Hospital Course section (see section 2.2) for the Discharge Summary note associated with the visit. • Extract Discharge Summary Addendums
Hospital Discharge Instructions	CS	• Not extracted.
Hospital Discharge Instructions	ToC, DP, CR, HIE (Inpatient only)	• Extract Discharge Information associated with the specific visits. • Extract Discharge Information Addendums

CCDA Module	CCDA Document	Data Extract
Immunizations	All	• Extract all patient refusals and all immunizations, including Immunizations 'due'. • Extract only the last two Influenza immunizations. • Extract Immunization Refused or Declined by the patient • Extract Immunizations Due
Medical Equipment	All	• Extract all active or expired Patient Implanted Devices
Medications	CS	• Extract all Active, Held, Suspended, and Pending Outpatient Prescriptions. • Extract all Given During Visit medications are extracted. • Extract all Outside Medications.
Medications	ToC, DP, CR	• Same as CS Medication but also include: • Extract recently expired (last 30 days) for chronic medications. • Inpatient (Unit Dose, IVs, Pending) that were Started between the Admit and Discharge (or Visit Date for ambulatory). • Extract all Historical Medications from past 5 years.
Medications	HIE	• Same as ToC/DP/CR but also include all Historical Medications from past 5 years.
Mental/Cognitive Status	CS	• Not extracted.
Mental/Cognitive Status	ToC, DP, HIE, CR	• Mini Mental Status Exam: Extract the most recent entry for the patient from the Measurement file. • Problems: Extract the subset of SNOMED codes determined to be related to cognitive status (EHR IPL COGNITIVE STATUS).
Patient	All	• Demographics for the requested patient.

CCDA Module	CCDA Document	Data Extract
Problems/Encounter Diagnoses	CS	• Extract Chronic, Episodic, and Sub-acute problems. • The CCDA Site Parameter ADD SOCIAL ENVIRONMENT PROB allows the sites to determine whether they want to extract social/environmental problems (see Section 3.1. • The CCDA Site Parameter ADD INACTIVE PERS HISTORY PROB allows the sites to determine whether they want to extract personal history with inactive status problems (see Section 3.1). • Extract any POVs for that Encounter (mark with an asterisk).
Problems/Encounter Diagnoses	ToC, DP, HIE, CR	• Extract chronic and sub-acute problems. • Extract social and environmental problems. • Extract personal history with inactive status problems. • Extract any POVs for that Encounter (mark with an asterisk).
Procedures	CS	• Extract the procedures done on today’s visit (V Procedure and V CPT). • Extract Radiology exams associated with the visit.
Procedures	ToC, DP, HIE, CR	• Extract all significant procedures for CPT codes entered in the APCH HS MAJOR PROCEDURES CPTS taxonomy. For ICD-9/ICD-10 codes, use the same ‘significant procedure’ logic as is used by the Health Summary. • Extract all Radiology exams for the patient.
Reason for Referral	CS	• Not extracted.
Reason for Referral	ToC, DP, HIE, CR	• Extract referral information for the referrals associated with the visits.

CCDA Module	CCDA Document	Data Extract
Reason for Visit/Hospitalization	CS, ToC	• Reason for Visit (Ambulatory), extract the Chief complaint. • Reason for Hospitalization (inpatient) get the Admit Diagnosis associated with the inpatient stay
Reason for Visit/Hospitalization	DP, CR	• Not extracted.
Results	CS	• Extract lab results that are modified or resulted. For ambulatory, extract labs resulted with the past 15 day for the date of the visit. For inpatient stays, extract all labs resulted during the inpatient stay. • Extract Radiology results for the current visit that has an impression and the report has been verified. For inpatient stay, only get the results of the first and last Radiology exam. • Extract Radiology Results with abnormal results that are within thirteen months of the earliest visit date. • Does not extract skin tests.
Results	ToC, DP, CR	• Extract resulted tests from Laboratory. For Ambulatory, results are not visit-specific. Extract the last two results for each atomic test and each panel that occurred within the last 30 days. For Inpatient, results are visit-specific. Extract the initial and last resulted test associated with the inpatient stay. • Extract Radiology results for the current visit that has an impression and the report has been verified. For inpatient stay, only get the results of the first and last Radiology exam. • Extract Radiology Results with abnormal results that are within thirteen months of the earliest visit date. • Extract skin tests that occurred in the previous year, except for the TB skin test that has no time limit.

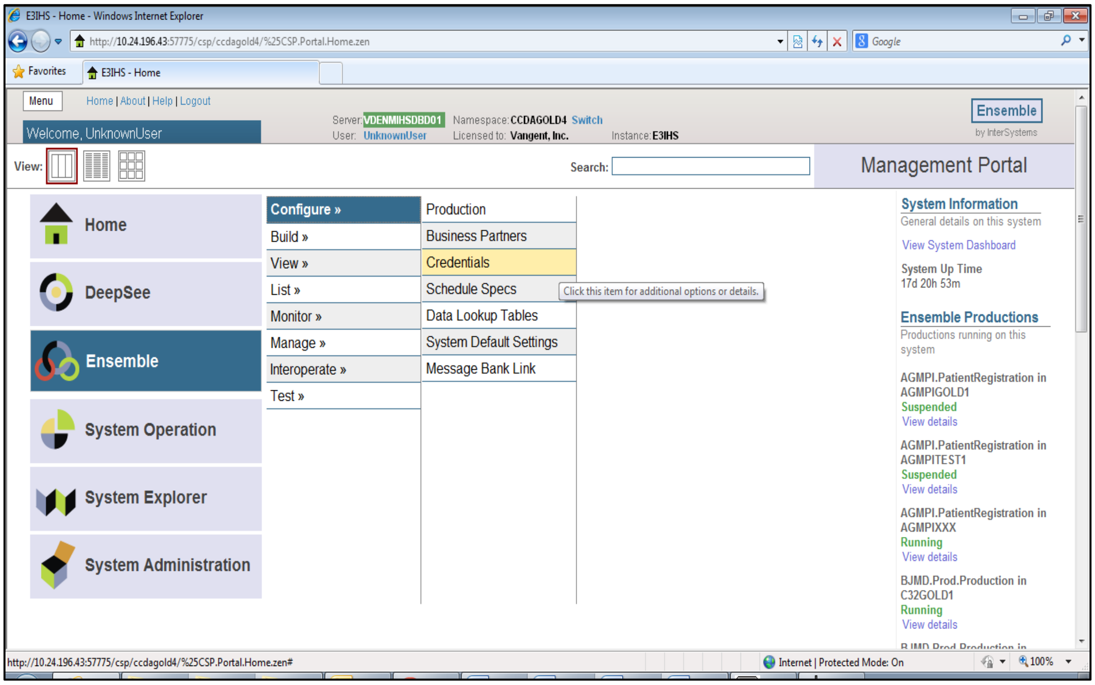
CCDA Module	CCDA Document	Data Extract
Results	HIE	• Extract resulted tests from Laboratory. For Ambulatory, results are not visit-specific. Extract the last five results for each atomic test and each panel that occurred within the last year. For Inpatient, results are visit-specific. Extract the initial and last three resulted test associated with the inpatient stay. • Extract Radiology results for the current visit that has an impression and the report has been verified. For inpatient stay, only get the results of the first and last Radiology exam. • Extract Radiology Results with abnormal results that are within thirteen months of the earliest visit date. • Extract skin tests that occurred in the previous year, except for the TB skin test that has no time limit.
Social History (Smoking Status)	All	• Get the most recent smoking status from V Health Factors.
Vital Signs	CS	• Get only the most recent three vital signs per type. Display only Height, Weight, Blood Pressure, and Body Mass Index (BMI).
Vital Signs	ToC, DP, CCD	• Extract measurements using the CCDA list of allowable measurements - Body Mass Index (BMI), Blood Pressure (BP), Head Circumference (HC), Height (HT), O2 Saturation (O2), Pulse (PU), Respiratory Rate (RS), Temperature (TMP), and Weight (WT). • For O2 Saturation measurement, also extract the Inhaled Oxygen Concentration, Inhaled Flow Rate, and Method modifiers. • Extract Pain measurement, even though it is not specified by CCDA. • Ambulatory vital signs are not visit-specific. Extract the last three measurements. • Inpatient vital signs are visit-specific. Extract the initial and last three associated with the inpatient stay.

7.0 Manage E-Mail Notifications

This step allows the user to configure the CCDA Ensemble production to automatically send e-mail notifications about new errors to select users. A notification is typically sent as soon as a new error occurs, but the number of e-mails is limited to one per 15 minutes in order to prevent flooding the recipients' mailboxes with multiple errors. This e-mail notification functionality is only available on systems that have an e-mail server configured. This managing e-mail notifications step is optional and may be skipped if the sites do not want to be notified about CCDA errors by e-mail. For requests coming from the EHR GUI, the site manager will be able to view errors in the CCDA Audit Log, which is described in the *CCDA Security Manual*, even if e-mail notifications are not set up.

Check if the site's e-mail server requires a user to sign on. If it does require a user to sign on, the credentials will need to be set up first. To set up the user credentials, sign on to HealthShare's Management Portal as an administrator and follow these instructions:

1. Switch to the CCDA namespace.
2. In the **Namespace Chooser** box, choose the appropriate CCDA namespace (the namespace will consist of "CCDA" concatenated with the name of the site's RPMS namespace).
3. On the **Management Portal** screen, click **Ensemble**, then click **Configure**, then click **Credentials**.



Server: VDENMIHSDBD01 Namespace: CCDAGOLD4 Switch
User: UnknownUser Licensed to: Vangent, Inc. Instance: E3IHS

System Up Time
17d 20h 53m

AGMPI.PatientRegistration in AGMPIGOLD1
Suspended

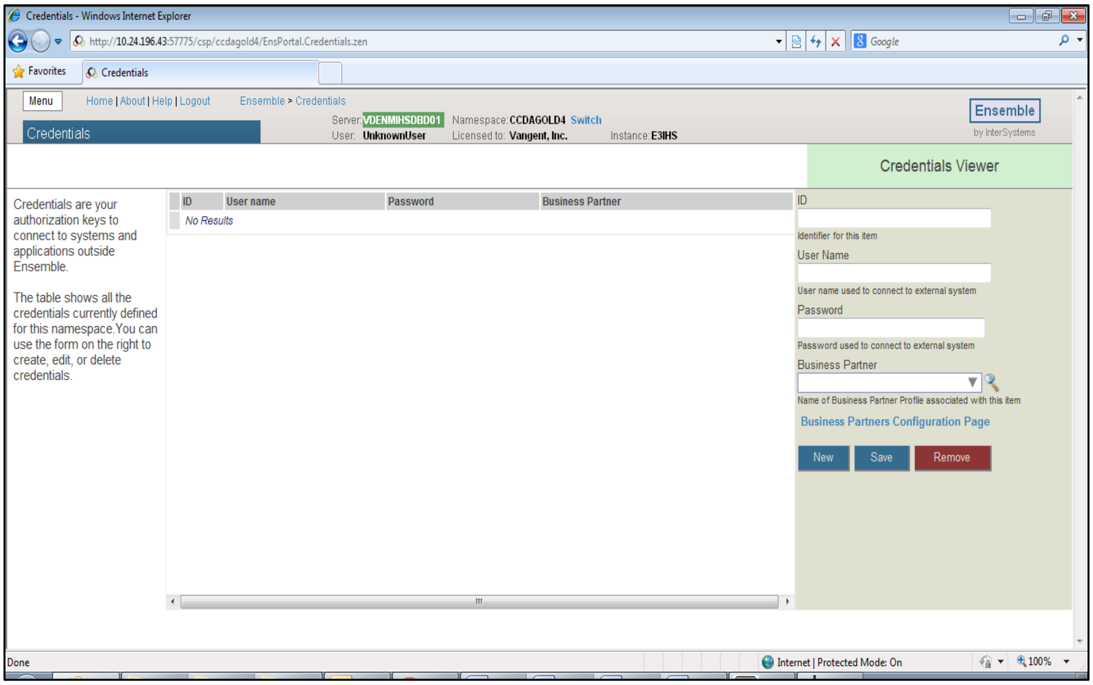
AGMPI.PatientRegistration in AGMPITEST1
Suspended

AGMPI.PatientRegistration in AGMPIXXX
Running

BJMD.Prod.Production in C32GOLD1
Running

Figure 7-1: Management Portal, Credentials option

Figure 7-2 shows the **Credentials Viewer** screen.


Credentials - Windows Internet Explorer
http://10.24.196.43:57775/csp/ccdagold4/EnsPortal.Credentials.zen
Google
Favorites
Credentials
Menu
Home | About | Help | Logout
Ensemble > Credentials
Credentials
Ensemble
by InterSystems
New
Save
Remove
Business Partners Configuration Page
Done
Internet | Protected Mode: On
100%

Server: VDENMIHSDBD01 Namespace: CCDAGOLD4 Switch
User: UnknownUser Licensed to: Vangent, Inc. Instance: E3IHS

Credentials Viewer

Credentials are your authorization keys to connect to systems and applications outside Ensemble.

The table shows all the credentials currently defined for this namespace. You can use the form on the right to create, edit, or delete credentials.

ID	User name	Password	Business Partner
No Results			

ID

Identifier for this item

User Name

User name used to connect to external system

Password

Password used to connect to external system

Business Partner

Name of Business Partner Profile associated with this item

Figure 7-2: **Credentials**

4. In the **ID** field enter an arbitrary ID that will identify the site's e-mail server, e.g., **mail-server** (this ID will later be utilized in the **Credentials** field of the e-mail notification screen).

5. In the **Username** field, the HealthShare username will be defaulted; however, change the HealthShare username to a valid username on the e-mail server that will allow the user to sign on to the server and send e-mails.

6. In the **Password** field, enter the password for the username that was entered in the previous step.

7. Leave the **Business Partner** field blank.

8. Click **Save** (the newly entered credential will be displayed in the list in the center of the screen).

9. Once the credentials have been configured (or if the site's e-mail server does not require authentication), sign onto HealthShare's Management Portal as the administrator.

10. Switch to the CCDA namespace. The namespace will consist of "CCDA" concatenated with the name of the site's RPMS namespace.

11. On the **Management Portal** page, click **Ensemble**, then click **Configure**, then click **Production**.

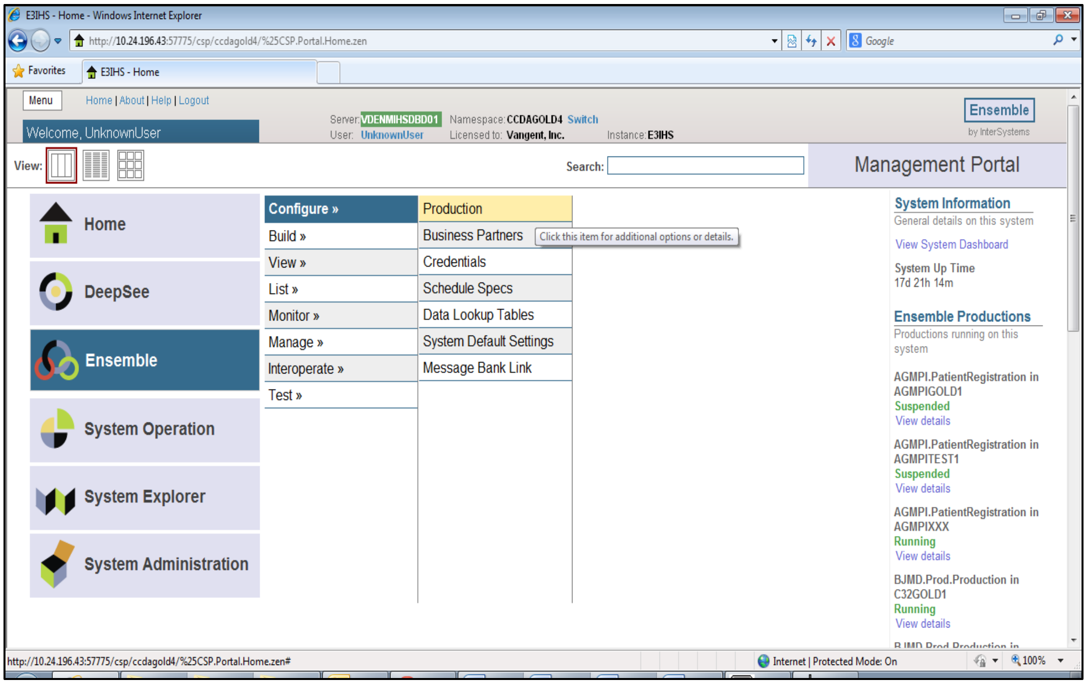
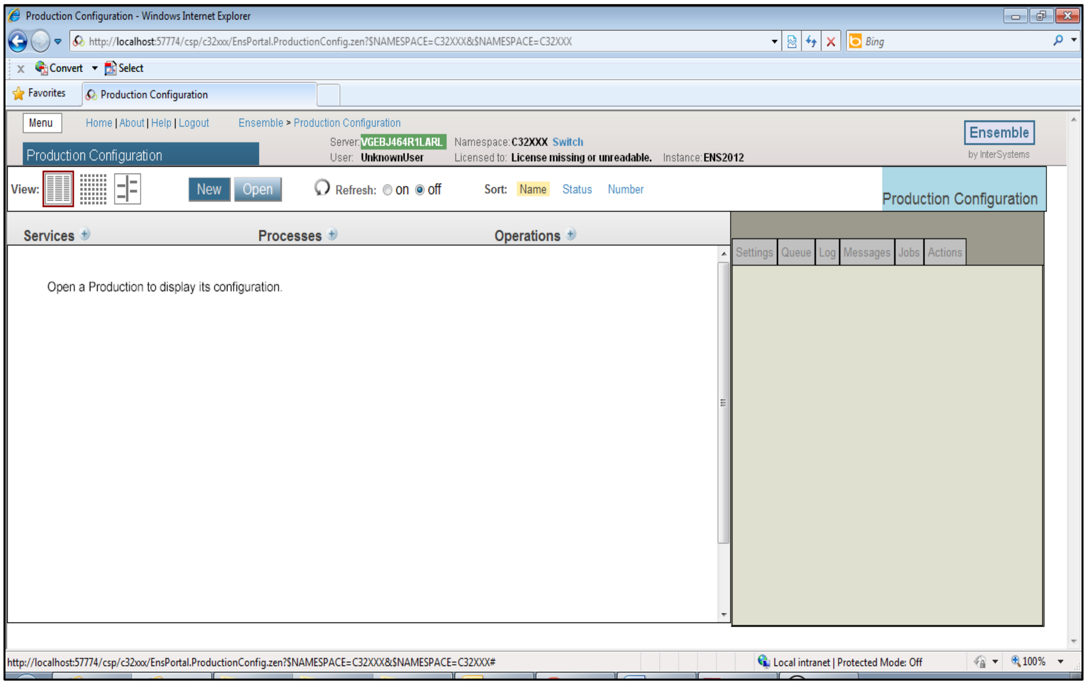

E3IHS - Home - Windows Internet Explorer
http://10.24.196.43:57775/csp/ccdagold4/%25CSP.Portal.Home.zen
Favorites
E3IHS - Home
Menu
Home | About | Help | Logout
Welcome, UnknownUser
Server VDENMIHSDBD01 Namespace: CCDAGOLD4 Switch
User: UnknownUser Licensed to: Vangent, Inc. Instance: E3IHS
Ensemble
by InterSystems
View:
Search:
Management Portal
Home
DeepSee
Ensemble
System Operation
System Explorer
System Administration
Configure »
Build »
View »
List »
Monitor »
Manage »
Interoperate »
Test »
Production
Business Partners
Credentials
Schedule Specs
Data Lookup Tables
System Default Settings
Message Bank Link
Click this item for additional options or details.
System Information
General details on this system
View System Dashboard
System Up Time
17d 21h 14m
Ensemble Productions
Productions running on this system
AGMPI.PatientRegistration in AGMPIGOLD1
Suspended
View details
AGMPI.PatientRegistration in AGMPITEST1
Suspended
View details
AGMPI.PatientRegistration in AGMPIXXX
Running
View details
BJMD.Prod.Production in C32GOLD1
Running
View details
http://10.24.196.43:57775/csp/ccdagold4/%25CSP.Portal.Home.zen#
Internet | Protected Mode: On
100%

Figure 7-3: **Management Portal, Production** option

12. On the **Production Configuration** screen, click **Open**.


Production Configuration - Windows Internet Explorer
http://localhost:57774/csp/c32xxx/EnsPortal.ProductionConfig.zen?$NAMESPACE=C32XXX&$NAMESPACE=C32XXX
Bing
Convert
Select
Favorites
Production Configuration
Menu
Home | About | Help | Logout
Ensemble > Production Configuration
Production Configuration
Server VGEBJ464R1LARL Namespace: C32XXX Switch
User: UnknownUser Licensed to: License missing or unreadable. Instance: ENS2012
Ensemble
by InterSystems
View:
New
Open
Refresh: ○ on ● off
Sort: Name Status Number
Production Configuration
Services
Processes
Operations
Settings
Queue
Log
Messages
Jobs
Actions
http://localhost:57774/csp/c32xxx/EnsPortal.ProductionConfig.zen?$NAMESPACE=C32XXX&$NAMESPACE=C32XXX#
Local intranet | Protected Mode: Off
100%

Open a Production to display its configuration.

Figure 7-4: **Production Configuration**, no production open

13. In the **Finder** dialog, click **BCCD**, then click **Prod**, then click **Production** to select the CCDA production (the **Production Configuration** screen will update to display the items for the CCDA production).

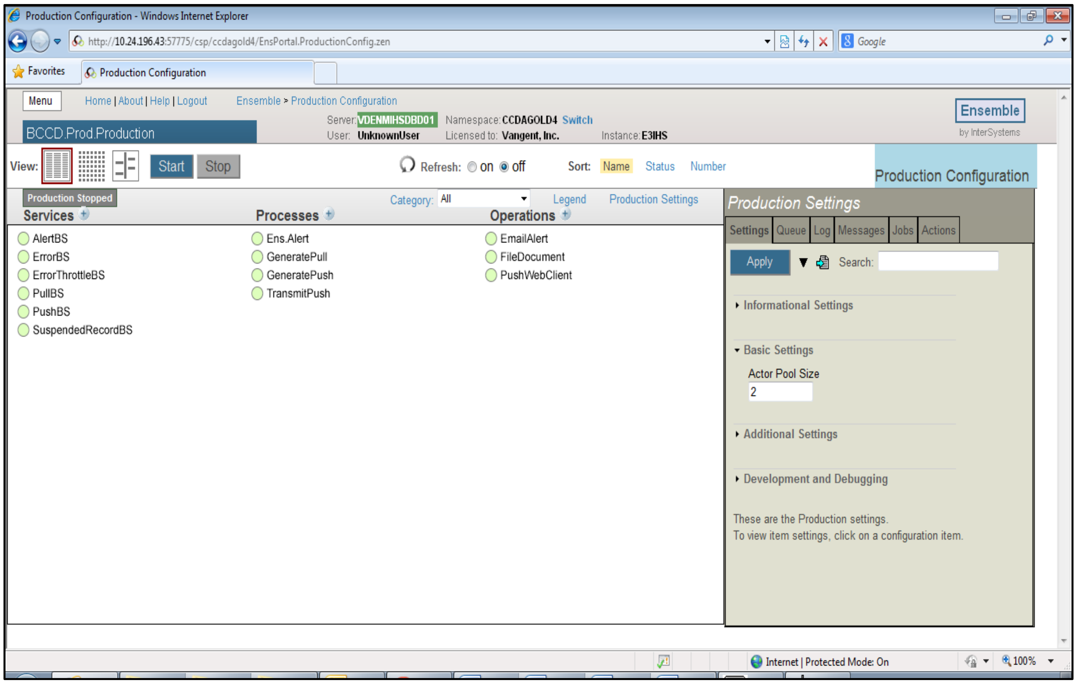


Figure 7-5: **Production Configuration**, CCDA production open

14. Single-click on **EmailAlert** in the **Operations** column (the details of this process will be displayed in the **Production Settings** box on the right side of the page).

15. In the **EmailAlert** box on the right-hand side, be sure the **Basic Settings** and **Additional Settings** sections are expanded, and then enter values in Table 7-1:

Table 7-1: **EmailAlert** settings

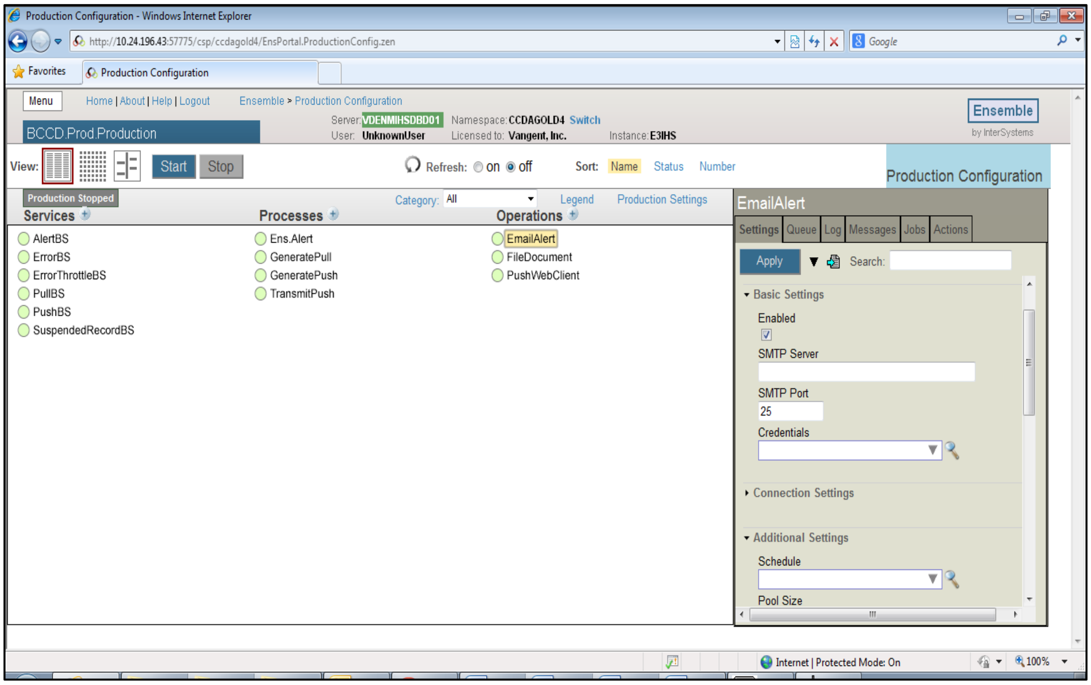
Field Name	Value
Enabled	Check the box to enable email alerts
SMTP Server	IP address or name of the email server at the site
SMTP Port	Port number used by the site's email server. The default is 25
Credentials	Only required if the e-mail server requires authentication (see instructions above)
Recipient	A comma-delimited list of email addresses that Ensemble will be sending alerts to, e.g., John.Doe@ihs.gov, Jane.Doe@ihs.gov
From	The e-mail address that the alerts will appear as coming from, e.g. CCDA@sitename.ihs.gov

If the site has a functional e-mail server but the user does not have some of the information in the **EmailAlert** settings table above, contact the Help Desk.

> **Note:** Do not modify any other values on this screen since it can invalidate the Ensemble production.

16. Once all the required data is entered, click **Apply** at the top of the **EmailAlert** box.

Figure 7-6 contains a sample screenshot which shows what the screen will look like during the configuration process.



BCCD.Prod.Production

Server: VDENMIHSDBD01 Namespace: CCDAGOLD4 Switch
User: UnknownUser Licensed to: Vangent, Inc. Instance: E3IHS

Refresh: ○ on ● off

Category: All

Enabled
☑

SMTP Server

SMTP Port
25

Credentials

Figure 7-6 : Ensemble e-mail server configuration

8.0 References and Sources

HL7 Implementation Guide for CDA Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use Release 2.1, August 2015: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=492

Office of the National Coordinator for Health Information Technology (ONC) 2015 Certification of Health Information Technology (CHIT): https://www.healthit.gov/topic/certification-ehrs/certification-health-it

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

BCCD

Namespace for CCDA files, routines and classes.

BMW

Namespace for classes generated from FileMan files.

Hypertext Transfer Protocol

A widely used communication protocol on the World Wide Web.

Simple Object Access Protocol

The communication protocol and message format used in communicating with web services.

Software Quality Assurance

The office within the IHS Office of Information Technology responsible for ensuring that the system conforms to RPMS Programming Standards and Conventions.

V Codes

V codes (codes V01–V91) are used to describe encounters with circumstances other than disease or injury. V codes are used either as a first listed (primary) or contributing (secondary) code depending on the situation.

Web service

An application programming interface (API) that allows communication with an application via SOAP messages over HTTP.

Web Service Description Language

A file that describes a web service’s API.

Acronym List

Acronym	Meaning
API	Application Programmer Interface
BMI	Body Mass Index
CCD	Continuity of Care Document
CCDA	Consolidated Clinical Document Architecture
CDA R2	Clinical Document Architecture Release 2
CHIT	Certified Health Information Technology
CPT	Current Procedural Terminology
CS	Clinical Summary
DP	Data Export, formerly Data Portability
DTL	Data Transformation Language
EHR	Electronic Health Record
GUI	Graphical User Interface
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level Seven
HTTP	Hypertext Transfer Protocol
I/T/U	IHS direct, tribal, and urban facilities. Generally, refers to all components of the Indian healthcare system
IHS	Indian Health Service
KIDS	Kernel Installation and Distribution System
OIT	Office of Information Technology
PHR	Personal Health Record
POV	Purpose of Visit
RPMS	Resource and Patient Management System
SAC	Standards and Conventions
SME	Subject Matter Expert
SNOMED CT	Systematized Nomenclature of Medicine--Clinical Terms
TB	Tuberculosis
ToC	Transitions of Care
WS	Web Service
WSDL	Web Services Description Language
XML	Extensible Markup Language

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