RESOURCE AND PATIENT MANAGEMENT SYSTEM

C32/CCD Clinical Summary

(BJMD)

User Manual

Version 1.0 Patch 3
September 2013

Office of Information Technology (OIT)
Division of Information Resource Management
Albuquerque, New Mexico

Preface

This manual provides information for site managers regarding operations of the C32/Continuity of Care Documents (CCD) Clinical Summary Version 1.0 (BJMD) package. This manual is not intended for end users of RPMS since there is no end user functionality in this package.

The BJMD package is designed to generate industry standard CCD in Healthcare Information Technology Standards Panel (HITSP) C32 format and transmit them to Indian Health Service (IHS) Health Information Exchange (HIE) and the Electronic Health Record (EHR) Graphical User Interface (GUI) using Web services.

Table of Contents

1.0 Introduction

The C32/Continuity of Care Documents (CCD) Clinical Summary (BJMD) software is a component of the Indian Health Service (IHS) Resource and Patient Management System (RPMS). It provides facilities for generating industry standard CCD in Healthcare Information Technology Standards Panel (HITSP) C32 format (version 2.5). CCD/C32 documents can be transmitted to IHS HIE C32 repositories or to the Electronic Health Record (EHR) Graphical User Interface (GUI) using Web services (WS). C32/CCD Clinical Summary documents will be referred to as "C32 documents" and the C32/CCD Clinical Summary software will be referred to as the "C32 software" in this document.

Although only C32 clinical summary documents are implemented in this release, there are a number of other HITSP-standard "C" documents that may be implemented within RPMS in the future. For this reason, the C32 management menu is called "C Messaging" and may be extended to support other C documents at a later time.

1.1 Purpose

C32 documents can serve a variety of purposes, including enabling clinician access to patient data in an emergency scenario, quality reporting, biosurveillance, patient access to their own data via a Personal Health Record (PHR) system, and medication/allergy reconciliation.

Each C32 document consists of two components: a human readable part known as a "Narrative Block," which can be displayed by any web browser, and a machine-readable part intended for automated data processing. The machine readable part may contain more detailed information than the human readable part.

1.2 Scope

A C32 document is an XML document summarizing current and pertinent historical information about an individual patient's healthcare record at a given facility. The current IHS implementation of the C32 standard (version 2.5) supports the following thirteen C32 modules:

- Allergies
- Conditions (Problems)
- Encounters
- Healthcare Providers
- Immunizations
- Information Source

- Insurance Providers
- Medications
- Person Information (Demographics)
- Procedures
- Results
- Support
- Vital Signs

2.0 Orientation

The following steps are needed to set up C32 at an RPMS site:

1. Enable Long Strings within Ensemble.
2. Create a directory for the C32 database.
3. Install the BFMC Kernel Installation and Distribution System (KIDS) build.
4. Confirm that the post-installation TaskMan task for BFMC has completed.
5. Install the BJMD KIDS build.
6. Encrypt the C32 database, if necessary.
7. Optionally set up e-mail notifications.
8. Turn off journaling for the C32 database and add it to the list of backed up databases.
9. Configure the C32 CSP application.
10. Set up site-specific C32 parameters.
11. Start C Messaging.

See the Installation Guide for details on the installation and configuration steps.

The C32 package has one RPMS menu used by site managers, **C MESSAGING MENU**, which comprises the following four menu options:

1. Edit C Messaging Site Parameters [BJMD EDIT SITE PARAMETERS].
2. Generate C32 for a single patient [BJMD C32ONEGEN].
3. Generate C32 documents for all patients in RPMS [BJMD C32ALLGEN].
4. Manage C Messaging transmissions [BJMD C MESS MGR].

The C32 package contains no menu options accessible by end users.

Site managers are responsible for performing the following tasks to ensure that C32 documents are successfully generated at their site:

1. Ensure that site-specific C32 parameters are set up appropriately–refer to Section 4.0.
2. Ensure that C Messaging is running–refer to Section 5.0.

3.0 C32 Architecture

Generation of C32 documents can be initiated in two ways. If EHR version 1.1 patch 8 or higher has been installed and configured at the site, then authorized EHR users will be able to request C32 documents for display within the EHR GUI client. If the site is a part of the IHS Health Information Exchange (HIE), then C32 documents will be generated nightly for all patients whose data has changed during the previous 24 hours and sent to HIE C32 repositories.

First, in order to accommodate requests from the EHR GUI, Ensemble has a Web service process listening for requests for C32 documents. When Ensemble receives a request, it creates a new entry in the C32 queue, records the ID of the patient for whom a C32 document was requested, and sets the entry status to **R** (for "Request").

Second, if a site is a part of the IHS HIE, then a nightly TaskMan task called **BJMD NHIE PUSH JOB** is automatically scheduled to run every night at the time specified by the site manager in menu option **Edit C Messaging Site Parameters**. When this task runs, it finds all patients whose data has changed since the last time it ran and creates new requests in the C32 queue.

> **Note**: When **BJMD NHIE PUSH JOB** runs for the first time, it creates new C32 requests for *all* patients in the RPMS database.

The only difference between C32 requests created by these two mechanisms is that requests created by **BJMD NHIE PUSH JOB** have a special flag in the body of the request so that Ensemble knows where to send the resulting C32 document.

The C32 queue is monitored by **BJMD BACKGROUND JOB**, another TaskMan task which serves as the main C32 generator. It is a persistent TaskMan task started at TaskMan startup time or manually from menu option **Manage C Messaging transmissions**. It constantly runs in the background until the site manager chooses to stop C Messaging. Once this TaskMan task finds a new C32 request with the status of **R** in the C32 queue, it changes the request's status to **CS** (for Compile Started.) It then extracts all relevant RPMS data for the specified patient and adds it to the body of the C32 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, **BJMD BACKGROUND JOB** changes the status of the request to **CE** (for Compile Ended). It then checks the C32 queue for other outstanding requests with the status of **R**. If it does not find any, then it goes into hibernation for anywhere between 0.1 and 2 seconds, the exact value depending on the site-specific C32 settings specified by the site manager as described in section 4.0.

The C32 queue is also monitored by the C32 Ensemble production running in the C32 namespace. When the C32 production finds a new request whose status is set to **CE**, it retrieves the C32 data from the body of the request and transforms it into a valid C32 document. It then transmits this document to its final destination using Web services and changes the status of the request to **T** (for "Transmitted").

If the site is a part of the IHS HIE, then the site manager has been provided with the URL of the associated C32 repository. Ensemble will use this URL to send C32 documents to the repository.

The main features of the C32 architecture at the sites that participate in the IHS HIE are:

- All C32 processing occurs at night, thus minimizing its impact on RPMS performance.
- All user requests for C32 documents are served by a separate C32 repository, thus insulating RPMS from potentially unpredictable load spikes.

4.0 Managing Site-Specific C32 Parameters

RPMS option **BJMD EDIT SITE PARAMETERS (Edit C Messaging Site Parameters)** allows site managers to configure site-specific C32 parameters at installation time and modify them if necessary. This menu option is locked by security key XUMGR, which site managers already have.

The following six fields can be edited using this option:

- BACKGROUND JOB DELAY
- RECORD GLOBAL REFERENCES
- TIME TO RUN NIGHTLY TASK
- DAYS KEEP TRANSMISSION ENTRIES
- REPOSITORY LOCATION
- ENABLED

The value of **BACKGROUND JOB DELAY** controls how long the C32 generator will be idle when there are no outstanding requests for C32 documents in the C32 queue. The default value is 1 second. The smaller this value, the faster the system will respond to incoming requests for C32 documents from the EHR GUI. On the other hand, if you set the value to 0.1 second, then the C32 generator will be checking the C32 queue 10 times every second, which can add an extra load to the server. Thus the site manager will have to maintain a balance between EHR GUI response time and the potential impact on RPMS performance. If you are not sure what to enter here, accept the default value of 1 second.

The value of **RECORD GLOBAL REFERENCES** is set to **Do not capture global references** by default and you should leave it that way. This value should *only* be changed if the Help Desk asks you to do so in order to help analyze performance issues. Setting this value to **Capture global references** can affect your disk space utilization and system performance.

The value of **TIME TO RUN NIGHTLY TASK** controls when the nightly background task (**BJMD NHIE PUSH JOB**) runs at night. If your site is not a part of the IHS HIE at this time, then leave this value blank. If your site is a part of the IHS HIE and you have been provided with the location of the off-site C32 repository, then enter the time when you want C32 documents to be generated and transmitted on a nightly basis. It is recommended that you enter a time outside of the regular business hours to minimize impact on the end users. This prompt accepts time values in all valid FileMan formats, e.g. **15:34** or **03:34PM**.

The value of **DAYS KEEP TRANSMISSION ENTRIES** determines how many days the C32 application will keep the intermediate compile structures created by BJMD BACKGROUND JOB. It is set to 30 days by default, but you can change it to any value between 7 and 9,999 days. The higher the number, the more disk space C32 will consume, as described in Section 3.2 of the C32 Installation Guide. On the other hand, if you set this number too low, the compile structures may be purged too soon and will not be available to facilitate debugging should any problems arise. If you are not sure what to enter here, keep the default value of 30 days.

The value of **REPOSITORY LOCATION** is the Universal Resource Locator (URL) of the outside C32 repository to which Ensemble sends C32 documents. If your site is not a part of the IHS HIE at this time, then leave the value of this field blank. If your site is a part of the IHS HIE and you have been provided with the location of the off-site C32 repository, then enter that location in this field. Should the location of the C32 repository assigned to your site change in the future, Area Support will notify you and provide the new location to enter here. Be extra careful when entering information in this field. A typo will prevent Ensemble from sending C32 documents to the repository.

Note: When you enter a URL into this field for the first time, C32 will generate C32 documents for *all* patients in the database, which can temporarily take up a lot of disk space. For this reason, when you enter the URL of the C32 repository at this prompt, the system checks how much free disk space the C32 database has. If you do not have enough disk space, you will see an error message when you try to enter a value in this field. If this happens, allocate more disk space for the C32 database as described in the Installation Guide and try again.

The value of the **ENABLED** field controls whether C32 documents are generated when C Messaging is running. Unless Support has instructed you otherwise, this value should always be set to **YES**.

Figure 4-1 contains a screen capture of a typical setup session with the user's entries in bold.

```
Select C Messaging Menu Option: edit  Edit C Messaging Site Parameters
Now editing C Messaging parameters:

BACKGROUND JOB DELAY: 1// <Enter>
RECORD GLOBAL REFERENCES: Do not capture global references
         // <Enter>
TIME TO RUN NIGHTLY TASK: 01:00AM

Now editing C32 (Patient Summary)-specific parameters:

DAYS KEEP TRANSMISSION ENTRIES: 30// <Enter>
REPOSITORY LOCATION: http://sample.ihs.gov:19090/PatientRecordReceiv
erService/PatientRecordReceiverService  Replace <Enter>
ENABLED?: NO// YES
```

Figure 4-1: Setting up C32 Site Parameters

5.0 Managing C Messaging

5.1 Starting and Stopping C Messaging

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

C Messaging should be running at all times, so there is no need to start or stop it manually once it has been installed. However, if the need arises, you can bring C Messaging up or down via the **Manage C Messaging transmissions** option, which is available in the **C Messaging Menu**. If this menu cannot be accessed from the regular **OPTION NAME** prompt in RPMS, then it will need to be added to your user settings.

If C Messaging is not running, you will be asked whether you want to start it as seen in Figure 5-1.

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

C Messaging processing task is not running

Start C Messaging? No// Y  (Yes)
```

Figure 5-1: Starting C Messaging

If C Messaging is running, then you will be asked whether you want to stop running the program.

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

C Messaging processing task is running

Stop C Messaging? No// Y  (Yes)
```

Figure 5-2: Stopping C Messaging

When you select the **Manage C Messaging transmissions** option, it performs a number of checks to see if there are any inconsistencies in site-specific C32 parameters. For example, Figure 5-3 contains the error message that will be displayed if you have entered the time for the nightly C32 upload process to run, but not the location of the repository to transmit C32 documents to.

```
Select C Messaging Menu Option: MAN  Manage C Messaging transmissions
C Messaging status:
```

```
Nightly Task is scheduled, but no Repository Location found for C32

C Messaging processing task is running

Stop C Messaging? No//
```

Figure 5-3: Sample inconsistency in site specific C32 parameters as reported when stopping C Messaging

5.2 Manually Generating One C32 Document

Ordinarily, C32 documents are generated automatically and the process does not require manual intervention. However, on occasion, you may be asked to regenerate the C32 document for one or more patients. When that happens, select the **Generate C32 for a single patient** option in the **C Messaging** menu. You will be asked to identify the patient by name, Social Security Number (SSN), date of birth, or chart number. If multiple patients match your input, you will be presented with a list similar to the one in Figure 5-4.

```
Select C Messaging Menu Option: ONE  Generate C32 for a single patient
ENTER NAME, SSN, DOB OR CHART#: SMITH,JOHN
   1    SMITH,JOHN                <A>   M 07-01-1987 XXX-XX-4901   CH
125315                                                              CI
125316                                                              URA
125317
   2    SMITH,JOHN                      M 12-29-1989 XXX-XX-7348   CH
139870                                                              CI
139871                                                              URA
139872
   3    SMITH,JOHN LANGDON       <WA>   M 02-04-1957 XXX-XX-8706   CH
105212                                                              CI
105213                                                              URA
105214
   4    SMITH,JOHN Z                    M 04-29-1969 XXX-XX-7636   CH
159349                                                          CI
159350(I)                                                           URA
159351
   5    SMITH,JOHN BRAD                 M 05-30-1989 XXX-XX-7775   CH
129483                                                              CI
129484                                                              URA
129485
ENTER '^' TO STOP, OR
CHOOSE 1-5: 2
  SMITH,JOHN                           M 12-29-1989 XXX-XX-7348   CH
139870                                                              CI
139871
```

```
                                                                    URA
139872
C32 request has been scheduled for patient SMITH,JOHN
```

Figure 5-4: Manually regenerating the C32 document for one patient

> **Note**: This menu option only works if your site is a part of the IHS HIE. If you try to access it at a site that is not a part of the IHS HIE, you will receive the error message shown in Figure 5.5.

```
Select C Messaging Menu Option: one  Generate C32 for a single patient
No receiving location is currently defined for C32 documents.
Your site needs to be associated with a receiving location in order
to be able to upload C32 documents. If Support has provided you with
the URL of your receiving location, please consult the C32 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 C Messaging on demand.
This will not affect other C Messaging functionality.
```

Figure 5-5: Error message displays when trying to manually regenerating a C32 document at a site that is not a part of the IHS HIE

5.3 Manually Regenerating All C32 Documents

If your site is a part of the IHS HIE, then, on rare occasions, the Help Desk may ask you to regenerate C32 documents for all patients in your database. When this happens, select the **Generate C32 documents for all patients in RPMS** option in the **C Messaging** menu. The system will check if you have enough disk space for this process and display the warning shown in Figure 5-6.

```
Select C Messaging Menu Option: all  Generate C32 documents for all
patients in RPMS
Checking free space...

Generation and transmission of C32 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 C32 documents will be done during the next C Messaging
nightly job which is currently scheduled to run at 23:40

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

Figure 5-6: Error message when trying to manually regenerate a C32 document at a site that is not a part of the IHS HIE

You will be asked to confirm that you really want to regenerate C32 documents for all patients.

If your site is not a part of the IHS HIE, the error message shown in Figure 5-7 will be displayed.

```
Select C Messaging Menu Option: all  Generate C32 documents for all
patients in RPMS
No receiving location is currently defined for C32 documents.
Your site needs to be associated with a receiving location in order
to be able to upload C32 documents. If Support has provided you with
the URL of your receiving location, please consult the C32 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 C Messaging on demand.
This will not affect other C Messaging functionality.
```

Figure 5-7: Error message when trying to manually regenerate all C32 documents at a site that is not a part of the IHS HIE

5.4 Managing C32 Ensemble Production

As described in Section 3.0 of this document, if your site is a part of the IHS HIE, C32 documents are sent to outside repositories using the C32 Ensemble production. In addition, if EHR version 1.1, patch 8 is installed and configured, then authorized EHR users can send requests for C32 documents to the C32 Ensemble production.

The C32 Ensemble production is automatically started when Ensemble starts up. During normal business operations, the C32 Ensemble production will remain running and will not require maintenance. If you ever find that you need to bring the C32 Ensemble production up or down manually, you will need to follow the instructions in Section 12.2 of the Technical Manual.

6.0 Auditing C32 Documents

The C32 application includes the C32 Audit Log. It allows site managers to retrieve audit information about specific requests for C32 data that come from the EHR GUI. The data elements available in the C32 Audit Log include the internal patient ID (DFN), the patient's full name, the status of the request for C32 data (Requested, Compile Started, Compiled Ended, Transmitted, Error), the time the request was received, and the time the C32 document was sent to the EHR GUI. In addition, the full text of the transmitted C32 document is available for viewing, both in human-readable and machine-readable (raw XML) formats. Site managers can search the C32 Audit Log data based on error status, the patient's first and last name, DFN and/or a range of request dates. Site managers can also limit the search to C32 requests that errored out.

The Audit Log is available at the following URL:
http://localhost:57772/csp/C32TST/BJMD.Audit.View.Log.cls, where:

1. **localhost** is the address of your RPMS server. If you are accessing the Audit Log from a different computer, you will need to use the IP address of the RPMS server
2. **57772** is the default port number used by Ensemble's System Management Portal. Check the URL of your System Management Portal for the port number used by your Ensemble instance.
3. **C32TST** is the name of the namespace where the C32 Ensemble production is running.

Once you access the Audit Log, you may want to bookmark the URL so that you will have ready access to it in the future. Figure 6-1 contains a sample C32 Audit Log page.

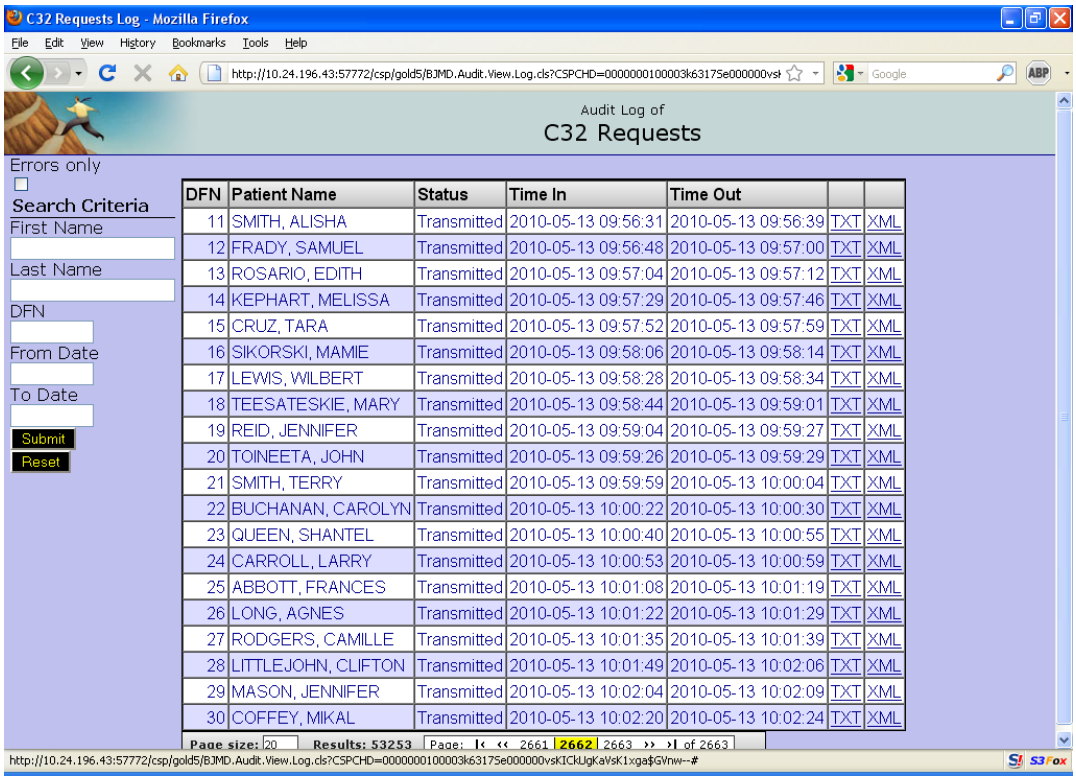

Figure 6-1:Sample C32 Audit Log

In addition, temporary compile structures are stored in the C32 application for a facility-defined period of time. These structures are stored in global ^BJMD.Xfer.QueueD and are meant to facilitate debugging in case of technical problems. There is no user interface to this global.

7.0 Limits on the Data Included in C32 Documents

C32 documents are supposed to contain "current and relevant historical" summary information about patients. For this reason, only recent clinical data is extracted from RPMS and included in C32 documents except as noted below.

The following list describes the time ranges used to extract RPMS data for individual C32 modules:

- Allergy, Condition, Healthcare Provider, Immunization, Procedure:
  - No time limit
- Encounter:
  - Less than two years old
- Insurance Provider:
  - Active insurance
- Medication:
  - Less than two years old
- Result (varies by result type):
  - Lab: Less than five years for most tests; no limit for tests whose Logical Observation Identifiers Names and Codes (LOINC) codes indicate that they never become obsolete, e.g. Human Immunodeficiency Virus (HIV) screening. In addition, the number of results is limited to the most recent 10 of each test name and the total number of results is limited to the most recent 1000, plus any “no limit” tests beyond the 1000 result limit.
  - Radiology: Less than five years old
  - Diagnostic Procedure: Less than five years old
  - Skin test: Less than five years old
  - Examinations: No time limit
  - Obstetrics (OB) Measurements: Less than 10 months old
- Vital Signs:
  - Less than two years old
  - Limited to the last 1,000

8.0 Managing E-mail Notifications

You can configure the C32 Ensemble production to automatically send e-mail notifications about new errors. 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 functionality is only available on systems that have an e-mail server configured. This functionality is optional and you do not need to configure it if you do not want to be notified about C32 errors by e-mail. You will still be able to view errors recorded while processing requests from the EHR GUI in the C32 Audit Log, which is described in Section 6.0.

The instructions for managing e-mail notifications depend on the version of Ensemble you are using. If you are using Ensemble 2009 or 2010, follow the instructions in section 8.1. If you are using Ensemble 2012, follow the instructions in section 8.2.

8.1 Ensemble 2009/2010

Check if your e-mail server requires you to sign on. If it does, you will need to set up credentials first:

1. Sign on to Ensemble's System Management Portal (SMP) as the administrator.
2. On the main **System Management Portal** page, select **Ensemble Management Portal** at the bottom of the leftmost column.
3. Select the appropriate C32 namespace from the drop-down list at the top of the page.
4. Click **Maintenance** in the list of options on the left side.
5. Click **Credentials** in the list of options on the left side.
6. Click **Create New Credentials** at the top of the screen. A new frame will appear at the bottom of the screen and you will be prompted to **Edit Credentials definition.** See Figure 8-1 for a sample screenshot. Your screen may look slightly different.

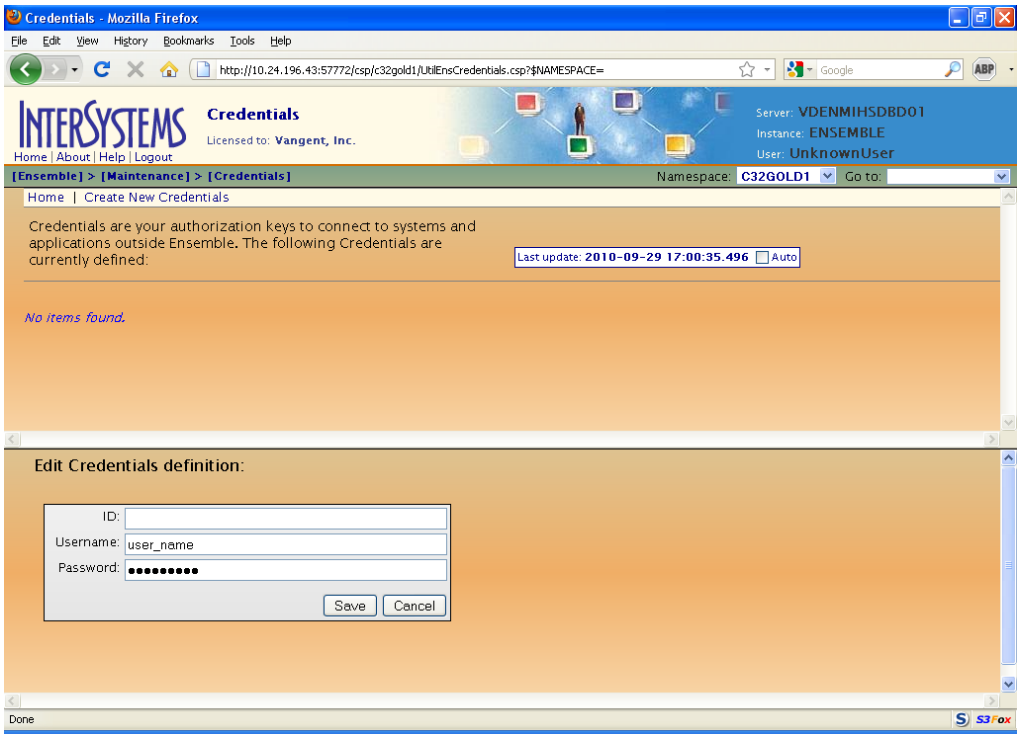

Figure 8-1: The **Credentials** window

7. In the **ID** field, enter an arbitrary ID that will identify your e-mail server, e.g., **mail-server**. You will later use this ID in the **Credentials** field of the **e-mail notification** screen.

8. In the **Username** field, your Ensemble user name will display as the default. Change it to a valid user name on the e-mail server, which will allow you to sign on to the server and send e-mails.

9. In the **Password** field, enter the password for the user name that you created in the previous step. If your screen contains a **Confirm Password** field, then re-enter the password in that field.

10. Click **Save**. The screen will be refreshed and you will see your newly entered user ID in the top portion of the screen.

Once you have configured credentials or confirmed that your e-mail server does not require credentials, sign on to Ensemble's System Management Portal as the administrator. You must use Internet Explorer (IE) and not another Web browser, because subsequent steps require Internet Explorer.

1. On the main **System Management Portal** page, select **Ensemble Management Portal** at the bottom of the leftmost column.

2. Select the appropriate namespace from the drop-down list at the top of the page. The page will refresh and the words **Ensemble Running** should display.

3. Click on the **more…** link next to the name of the running production ("BJMD.Prod.Production"). The **Ensemble Productions** page will display.

4. Click the **Configure** link on the right side. The **Ensemble Configuration** page will display and, after a brief delay, a graphical representation of the C32 production will display. The top block on the right, under **Business Operations**, should read **AlertEmailBO**.

5. Click **AlertEmailBO** and the details of this process will display at the bottom of the page.

6. In the **Specific Settings** column on the right side, enter values in the following fields:

Table 8-1: E-Mail Notification Values

Field Name	Value
SMTP Server	IP address or name of the e-mail server at your site.
SMTP Port	Port number used by your e-mail server. The default is 25.
Credentials	Only required if the e-mail server requires authentication (refer to instructions above).
Recipient	A comma-delimited list of e-mail 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. c32@ihs.gov.

If you have a functional e-mail server but do not have some of this information, contact the Help Desk. Do not modify any other values on this screen because it can invalidate the Ensemble production. Once you have entered all required data, click **Apply** at the top of the lower frame.

Figure 8-2 contains a sample screenshot that shows what the page will look like during the configuration process.

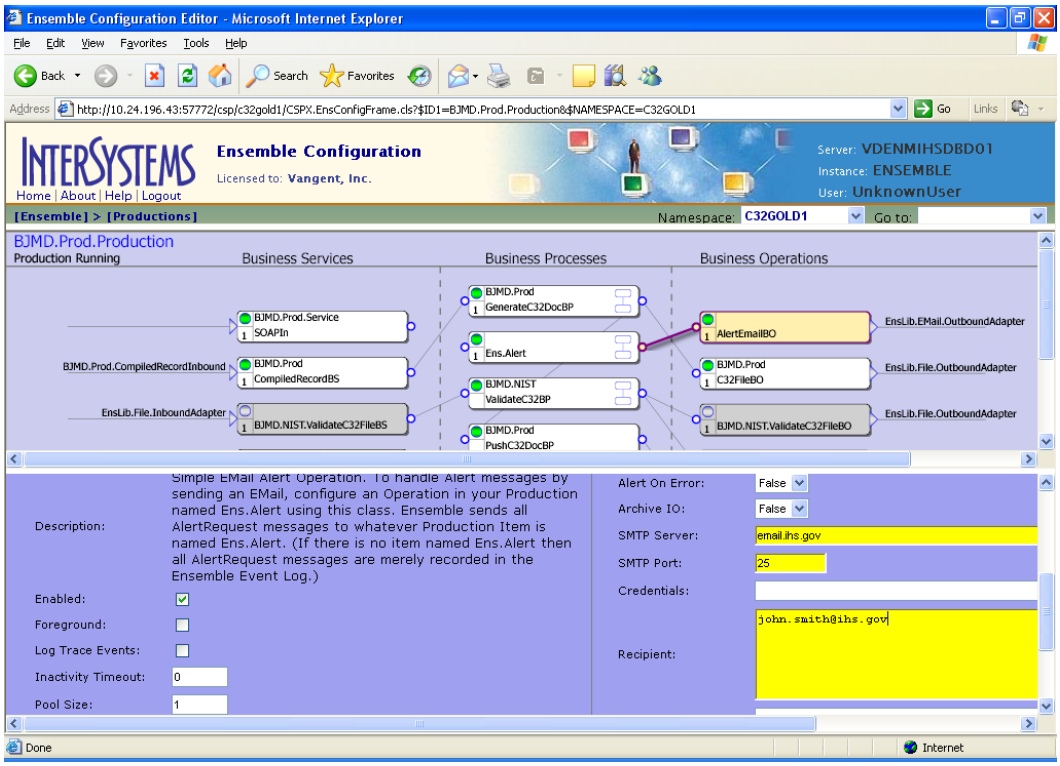

Figure 8-2: E-mail notifications in an Ensemble production

8.2 Ensemble 2012

Check if your e-mail server requires you to sign on. If it does, you will need to set up credentials first:

1. Sign on to Ensemble's Management Portal as the administrator.

2. At the top center, the main **Management Portal** page displays the server name, the current user, the current namespace, license and instance information, and a **Switch** link. Click the **Switch** link.

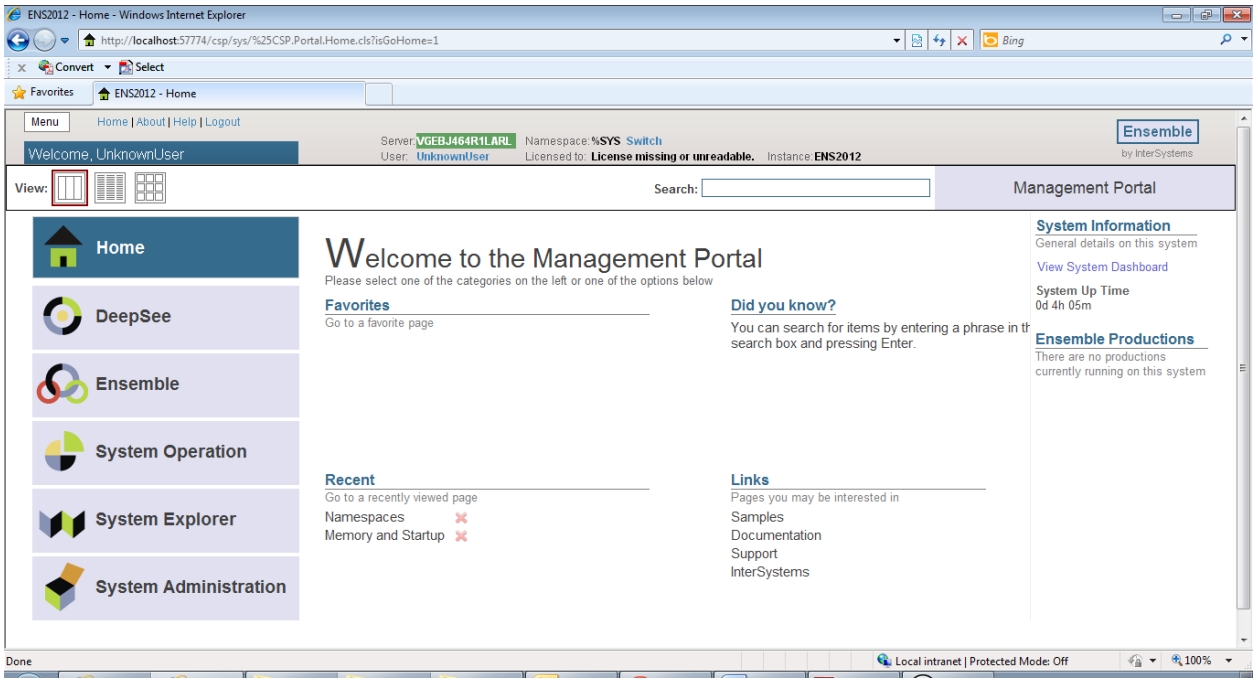

Figure 8-3: Management Portal

3. In the **Namespace Chooser** box, select the appropriate C32 namespace. The namespace will consist of "C32" concatenated with the name of your RPMS namespace. For example, if your RPMS namespace is called "TEST5", then the associated C32 namespace will be called "C32TEST5". Click **OK** to select the namespace. The namespace displayed on the **Management Portal** will be updated to reflect your selection.

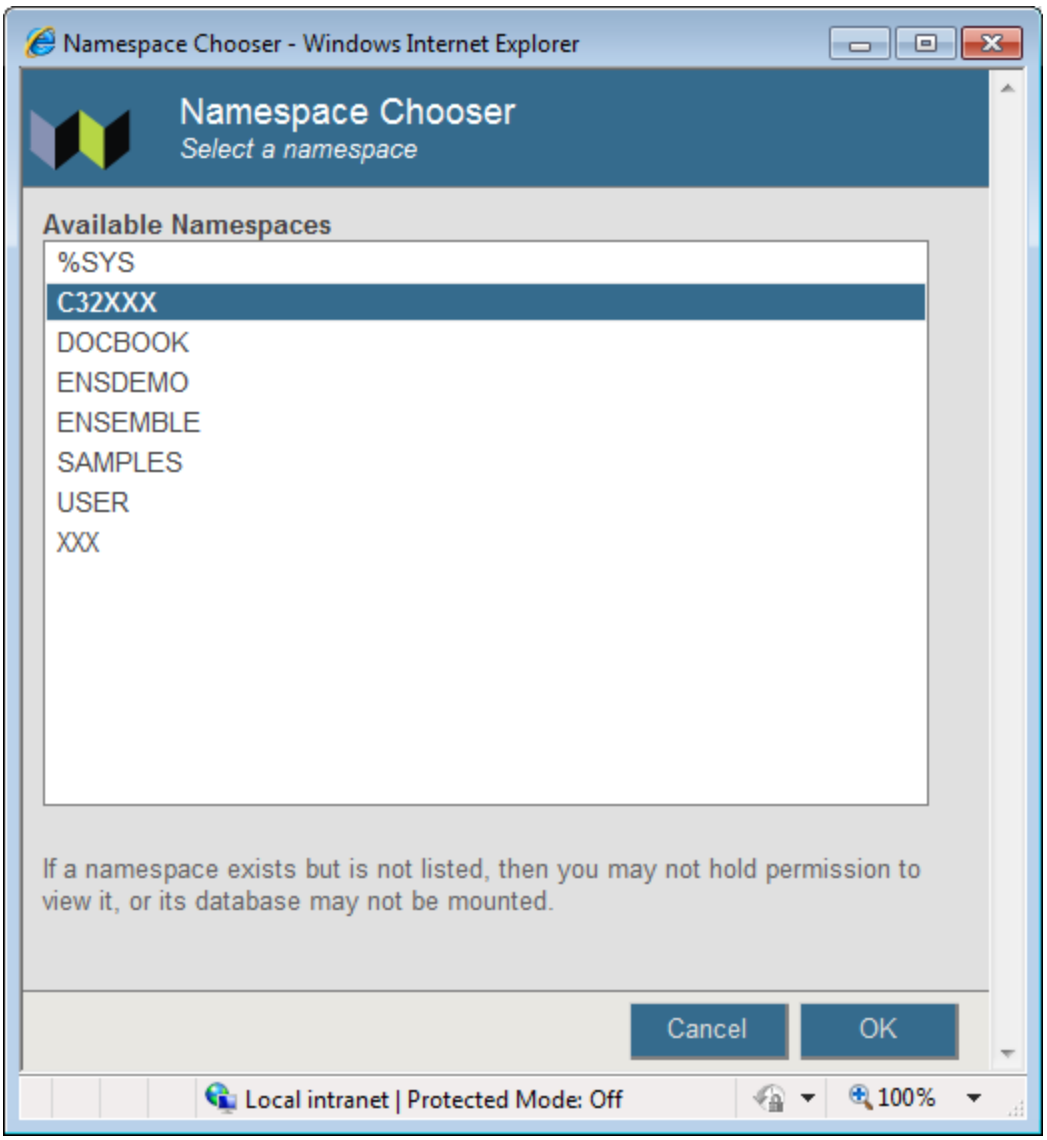

Figure 8-4: Namespace Chooser

4. In the **Management Portal**, click **Ensemble**, then click **Configure** >>, then click **Credentials**.

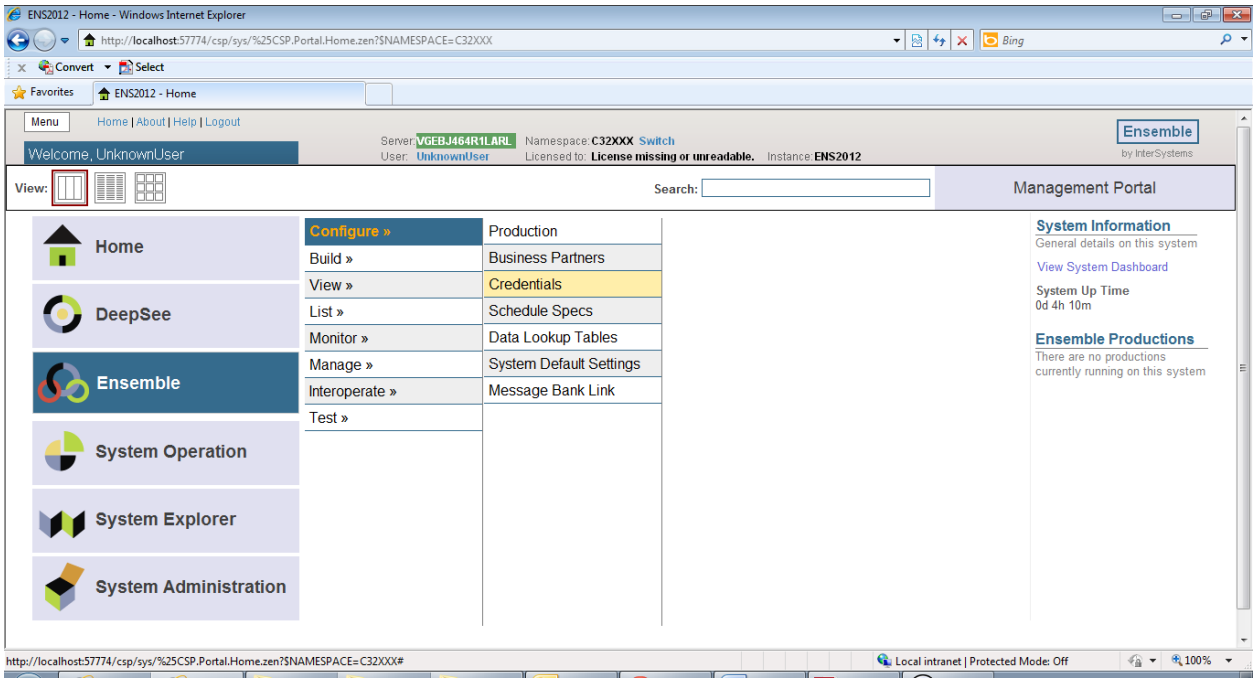

Figure 8-5: Management Portal

You will now be viewing the **Credentials Viewer** screen.

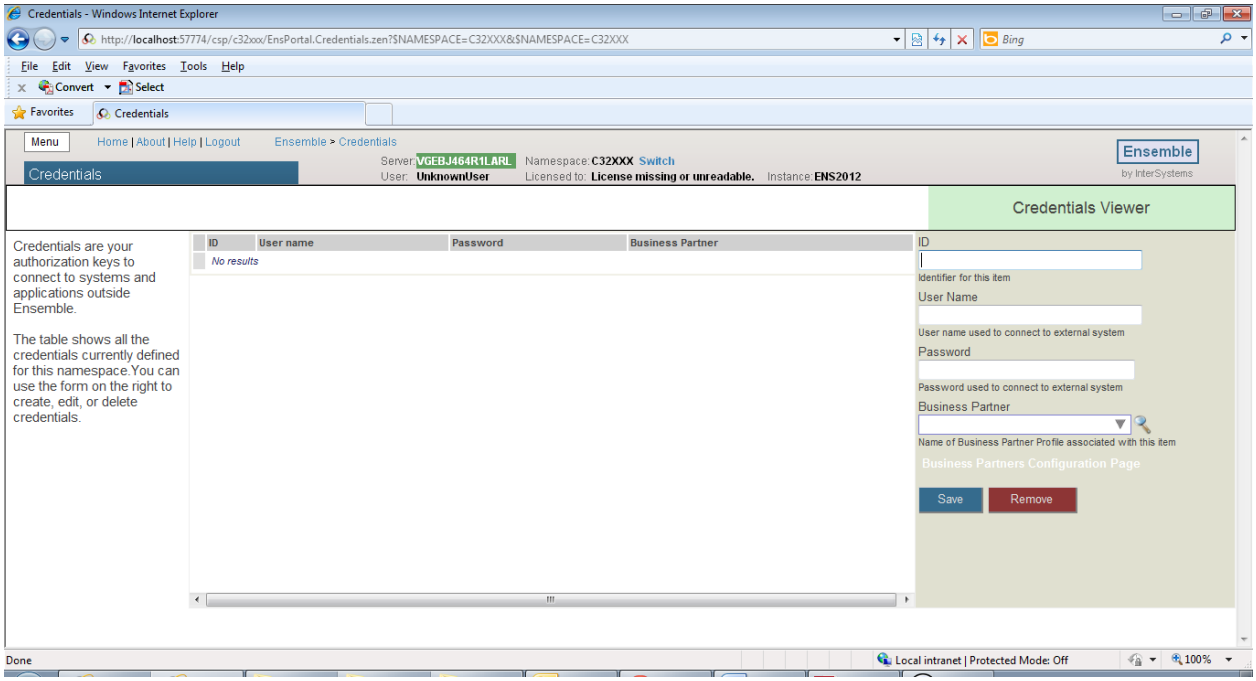

Figure 8-6: Credentials Viewer

5. In the **ID** field, enter an arbitrary ID that will identify your e-mail server, e.g., **mail-server**. You will later use this ID in the **Credentials** field of the **e-mail notification** screen.

6. In the **Username** field, your Ensemble user name will display as the default. Change it to a valid user name on the e-mail server, which will allow you to sign on to the server and send e-mails.

7. In the **Password** field, enter the password for the user name that you created in the previous step.

8. Click **Save**. The screen will be refreshed and you will see your newly entered user ID in the center of the screen.

Once you have configured credentials or confirmed that your e-mail server does not require those, sign on to Ensemble's Management Portal as the administrator.

1. At the top center, the main **Management Portal** page displays the server name, the current user, the current namespace, license and instance information, and a **Switch** link. Click the **Switch** link.

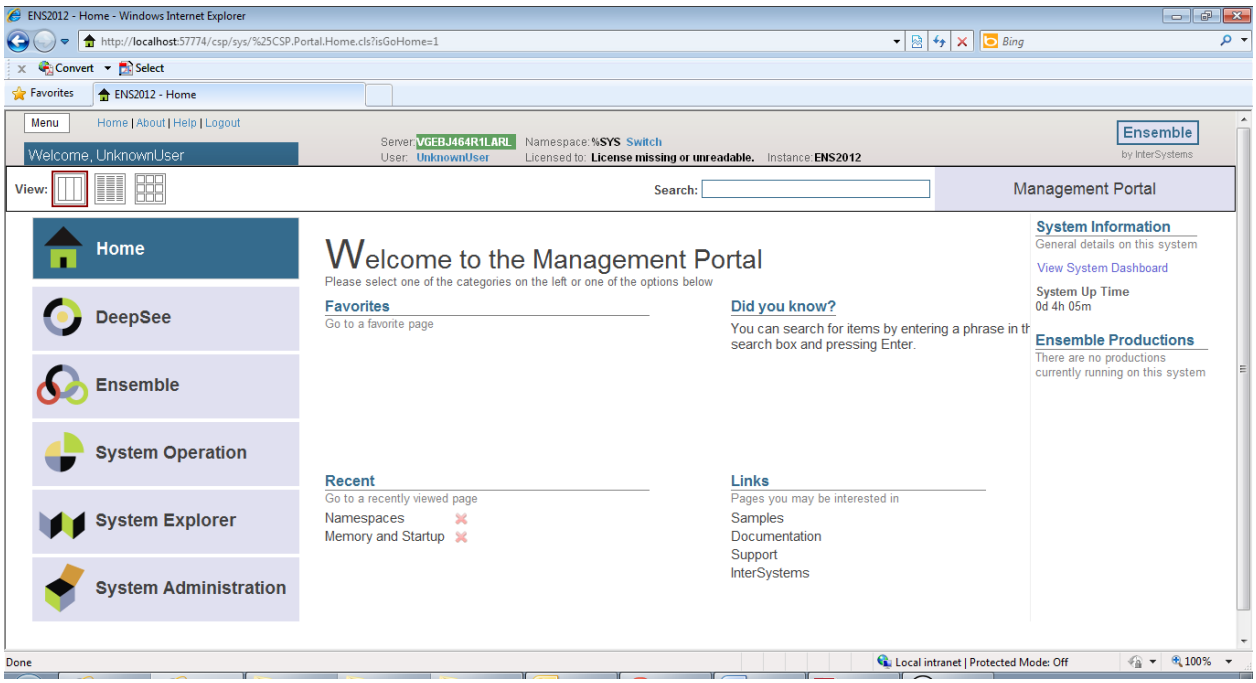

Figure 8-7: Management Portal

In the **Namespace Chooser** box, select the appropriate C32 namespace. The namespace will consist of "C32" concatenated with the name of your RPMS namespace. For example, if your RPMS namespace is called "TEST5", then the associated C32 namespace will be called "C32TEST5". Click **OK** to select the namespace. The namespace displayed on the **Management Portal** will be updated to reflect your selection.

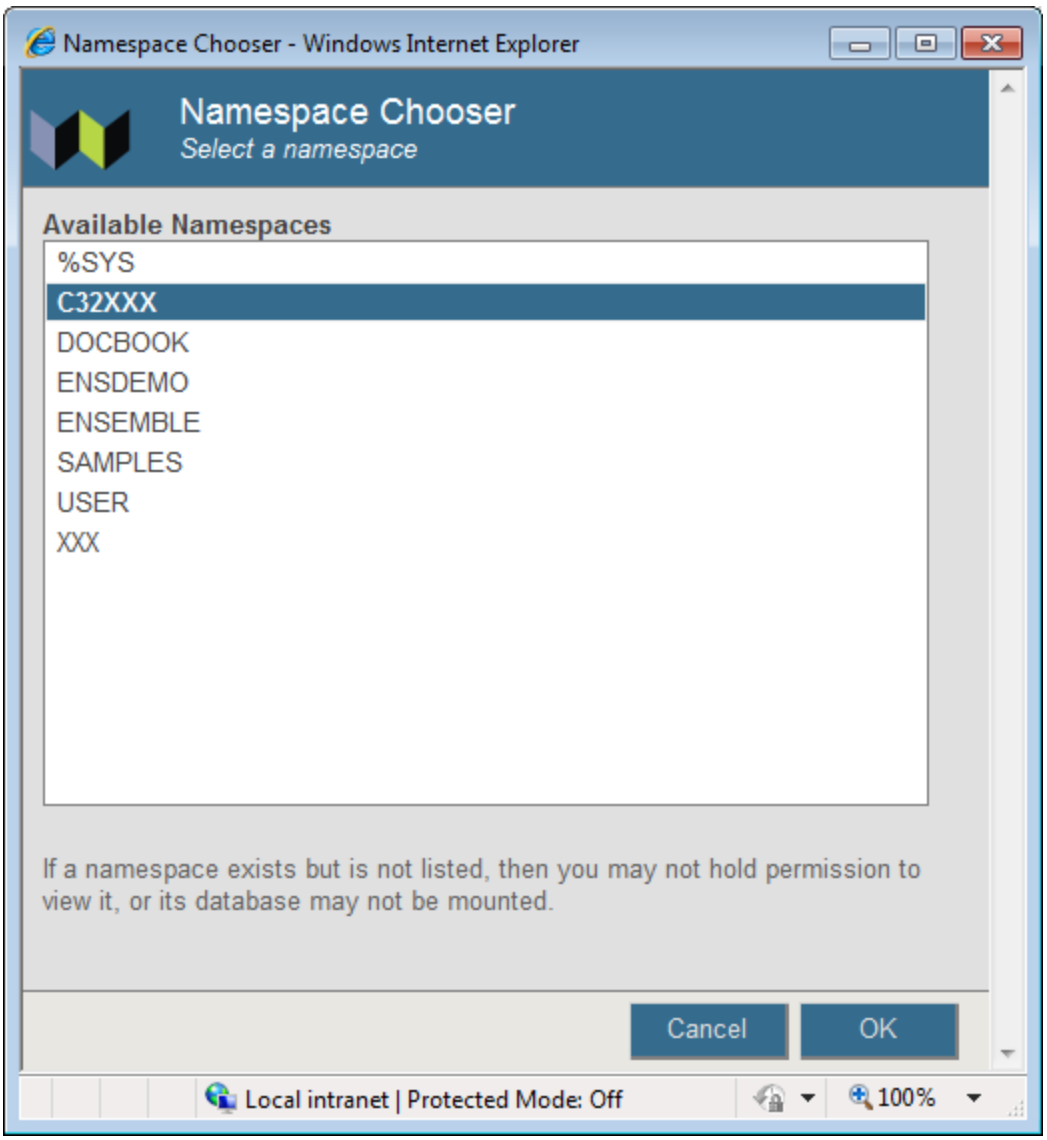

Figure 8-8: Namespace Chooser

1. In the Management Portal, click **Ensemble**, then click **Configure** >>, then click **Production**.

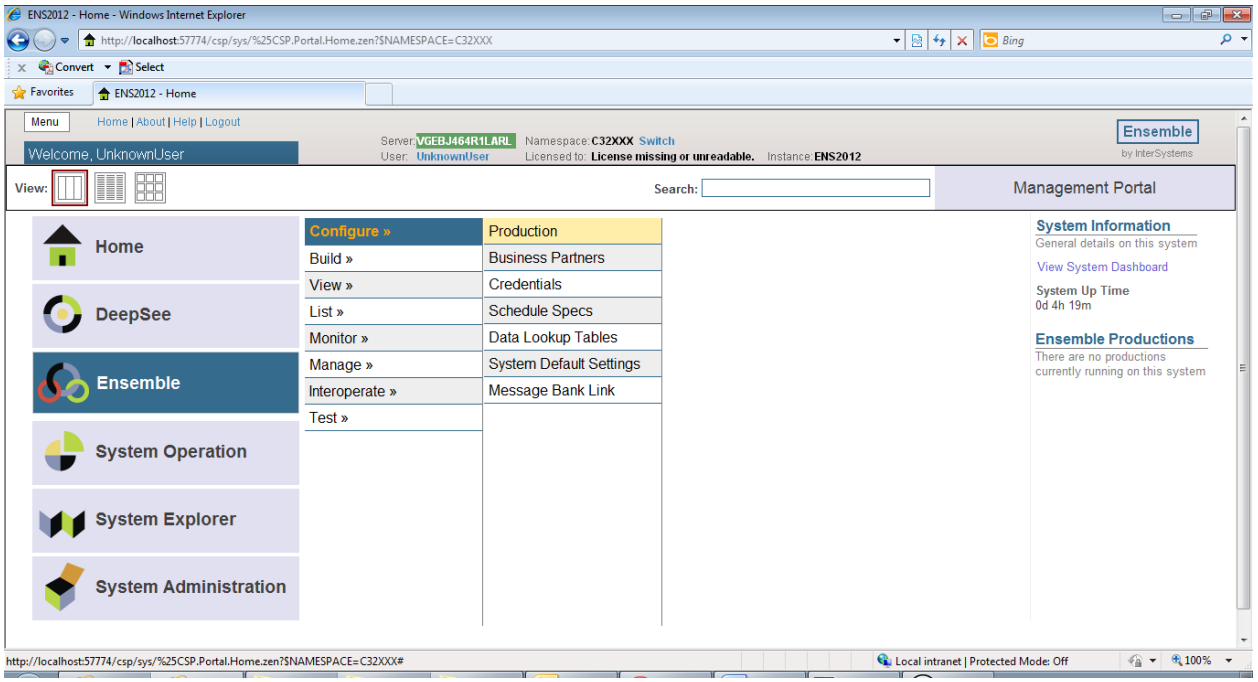

Figure 8-9: Management Portal

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

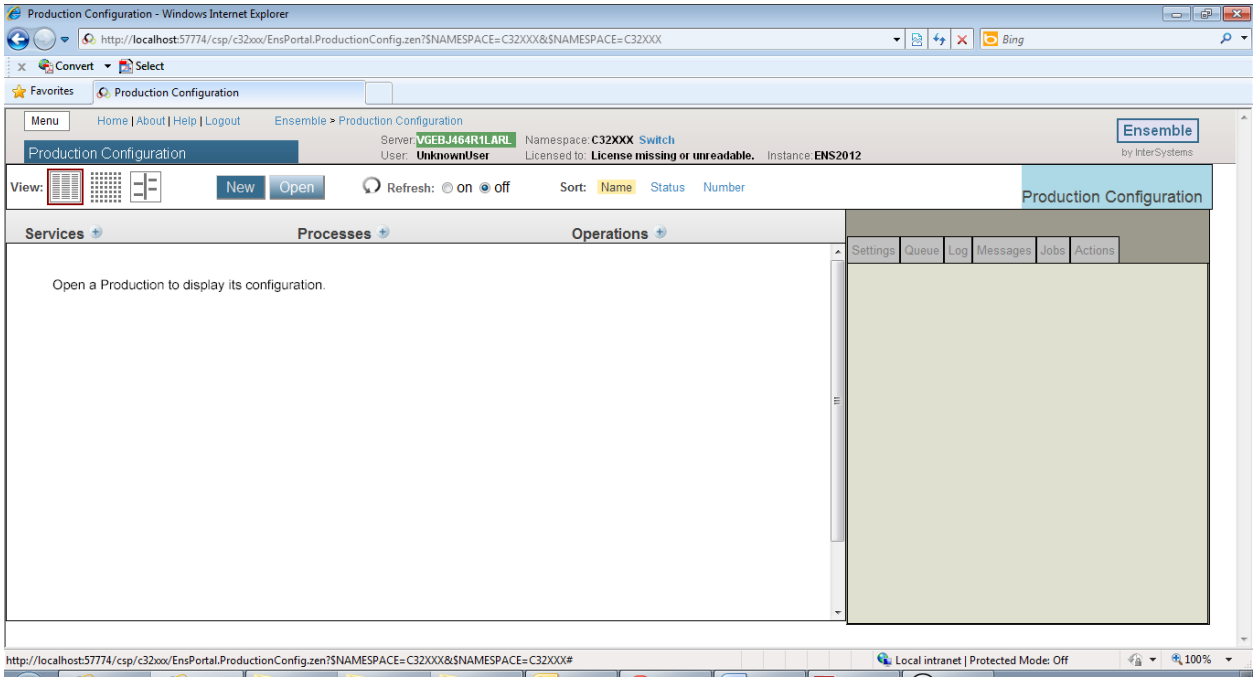

Figure 8-10: Production Configuration

3. In the **Finder Dialog**, click **BJMD**, then click **Prod**, then click **Production** to select the C32 production.

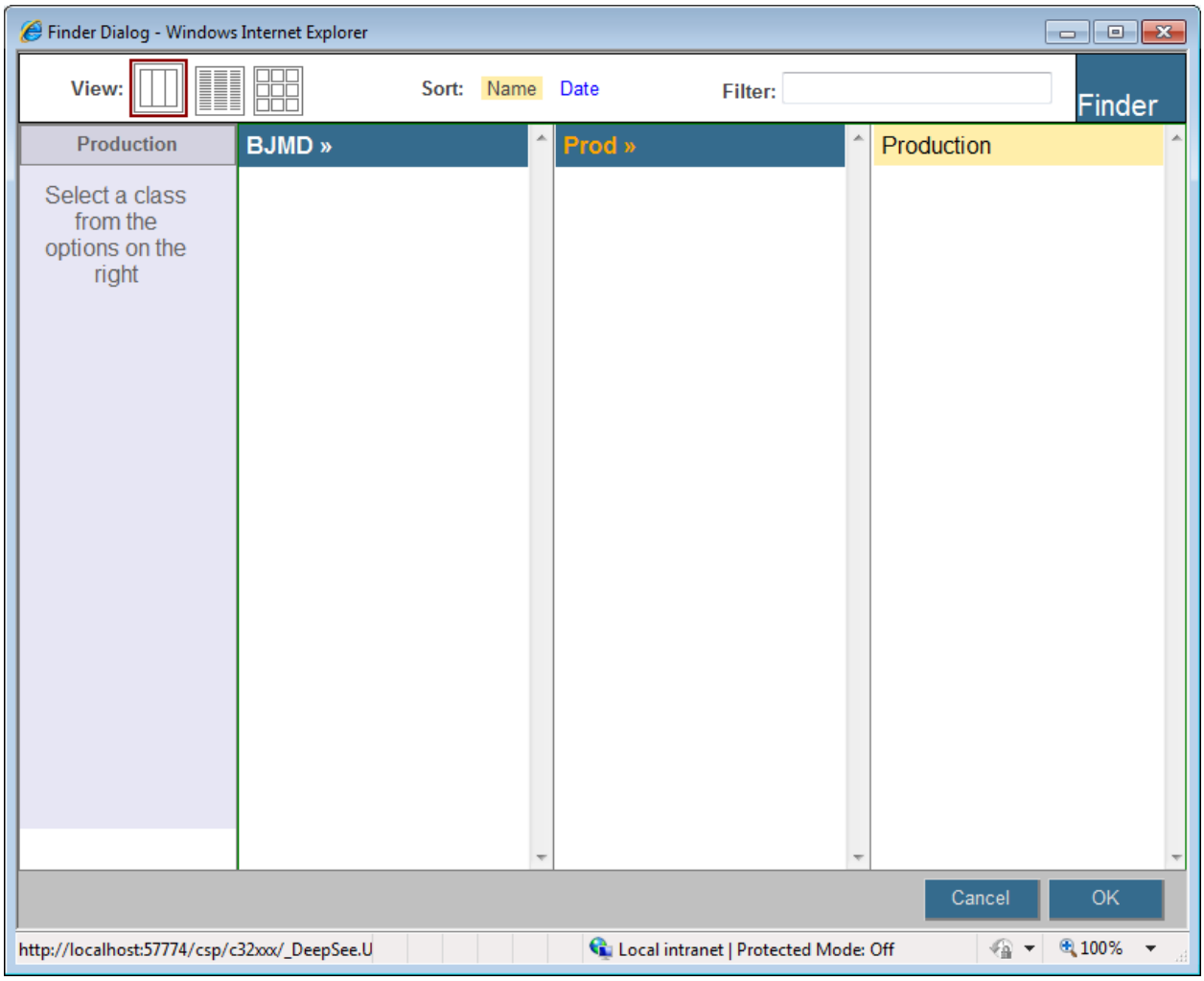

Figure 8-11: Finder Dialog

4. The **Production Configuration** screen will update to display the items for the C32 production.

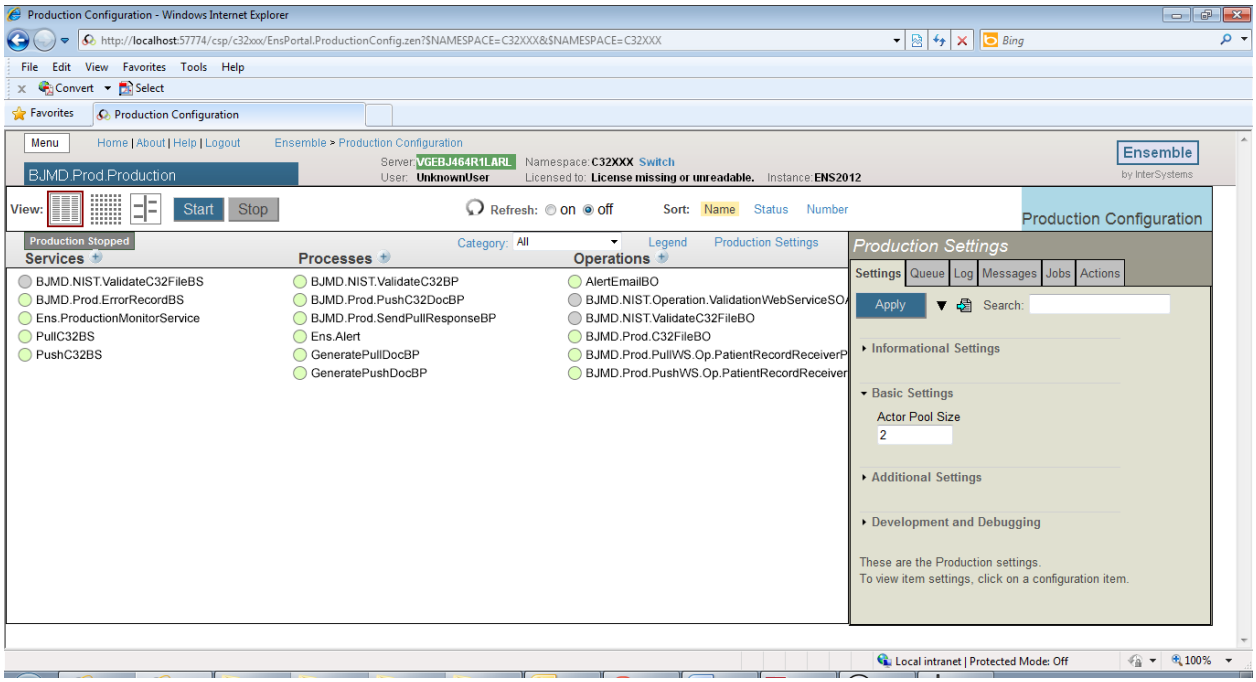

Figure 8-12: Production Settings

1. Single-click on **AlertEmailBO** in the **Operations** column. The details of this process will be displayed in the **Production Settings** box on the right side of the page.

2. In the **AlertEmailBO** box on the right-hand side, make sure that the **Basic Settings** and **Additional Settings** sections are expanded, then enter values in the following fields:

Table 8-2: E-Mail Notification Values

Field Name	Value
SMTP Server	IP address or name of the e-mail server at your site.
SMTP Port	Port number used by your e-mail server. The default is 25.
Credentials	Only required if the e-mail server requires authentication (refer to instructions above).
Recipient	A comma-delimited list of e-mail 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. c32@ihs.gov

If you have a functional e-mail server but do not have some of this information, contact the Help Desk. Do not modify any other values on this screen because it can invalidate the Ensemble production. Once you have entered all required data, click **Apply** at the top of the lower frame.

Figure 8.13 contains a sample screenshot that shows what the page will look like during the configuration process.

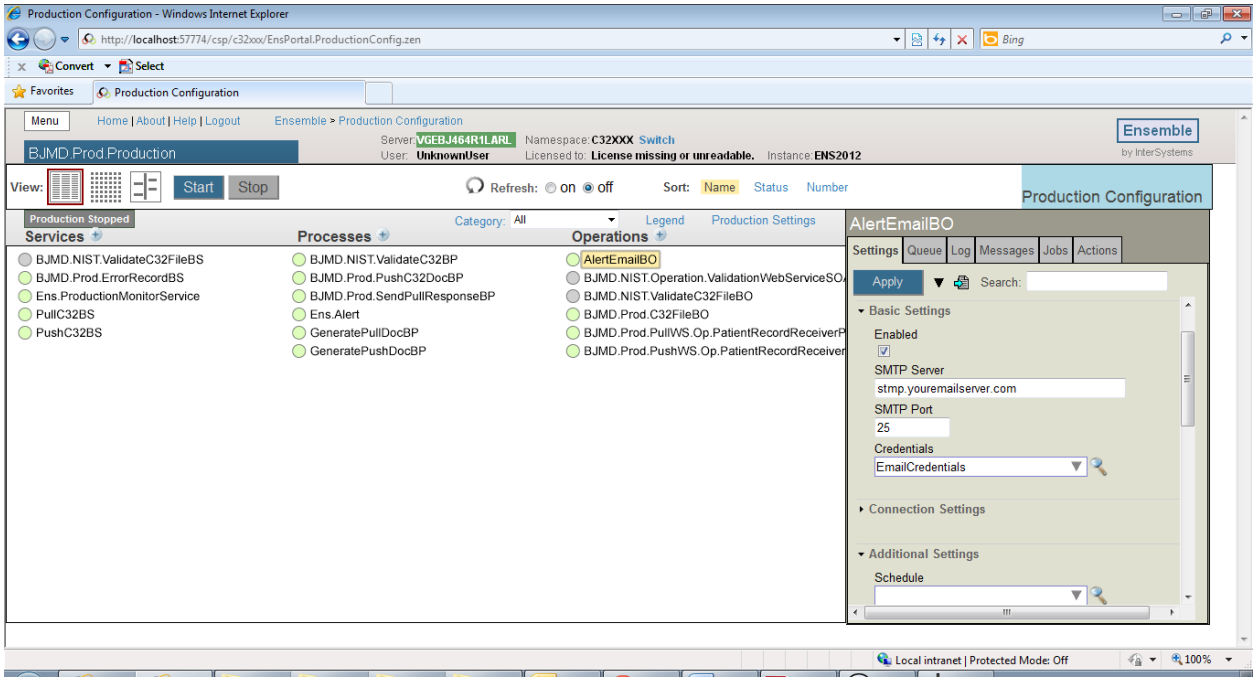

Figure 8-13: E-mail notifications in an Ensemble production

9.0 References and Sources

Version 2.5 of C32–HITSP Summary Documents Using HL7 CCD Component standard specification at: http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=4&PrefixNumeric=32 .

Appendix A: RPMS Rules of Behavior

The Resource and Patient Management System (RPMS) 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: http://security.ihs.gov/.

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

API

Application Programmer Interface

BFMC

Namespace for classes generated from FileMan files

BJMD

Namespace for C32 files, routines, and classes.

CCD

Continuity of Care Document.

CDA R2

Clinical Document Architecture Release 2

DTL

Data Transformation Language

FM2C

FileMan-to-Class mapper. Prior to version 1.0, the acronym stood for FileMan-to-Caché mapper.

GOTS

Government off the Shelf. Refers to existing Government-owned and developed software applications.

GUI

Graphical User Interface

HITSP

Healthcare Information Technology Standards Panel.

HRSA

Health Resources and Services Administration. An agency within the Department of Health and Human Services.

I/T/U

Abbreviation referring to all IHS direct, tribal, and urban facilities. Using the abbreviation I/T/U generally refers to all components of the Indian healthcare system.

IHS

Indian Health Service

ITSC

Information Technology Support Center. Currently referred to as Office of Information Technology (OIT).

KIDS

Kernel Installation and Distribution System.

NIST

National Institute of Standards and Technology

OIT

Office of Information Technology. The organization within IHS that is responsible for developing and maintaining RPMS and related IT functions.

PCC

RPMS Patient Care Component Refers to functions within RPMS as a clinical data repository, storing visit-related data about a patient.

PCC form

The paper form used in most I/T/U clinics on which the provider(s) document all data from the patient's visit. Used by data entry staff to enter patient data into RPMS PCC.

PCC+

The RPMS PCC+ software produces automated, customizable PCC forms.

PHR

Personal Health Record.

RPMS

Resource and Patient Management System. A series of integrated software components that includes clinical, administrative, and financial functions.

SAC

Standards and Convention

SQA

Software Quality Assurance. The office within OIT responsible for ensuring that the system conforms to RPMS Programming Standards and Conventions.

SRD

Software Requirements Document

Taxonomy

In RPMS, a grouping of functionally related data elements, such as ICD codes. For C32, taxonomies will be used to list procedures, test results and other data elements with non-standard data extraction criteria.

TuneTable

A Caché utility class which optimizes subsequent query performance by examining a persistent class' data and setting class selectivity and extent size.

UI

User Interface

WS

Web Services

XML

Extensible Markup Language

Contact Information

If you have any questions or comments regarding this distribution, please contact:

Phone: **(505) 248-4371 or (888) 830-7280 (toll free)**

Fax: **(505) 248-4363**

Web: http://www.ihs.gov/GeneralWeb/HelpCenter/Helpdesk/index.cfm

Email: support@ihs.gov

Trademark Notice

Caché and Ensemble are registered trademarks of InterSystems Corporation.

Continuity of Care Document (CCD) is a registered trademark of Health Level Seven International.

Internet Explorer is a registered trademark of Microsoft Corporation.