



RESOURCE AND PATIENT MANAGEMENT SYSTEM

# **Electronic Health Record**

(EHR)

## **Implantable Device List (IDL) Component Addendum to User Manual**

Version 1.1 Patch 29  
September 2020

Office of Information Technology  
Division of Information Technology

# Table of Contents

<b>1.0</b>	<b>Introduction.....</b>	<b>1</b>
<b>2.0</b>	<b>Implantable Device .....</b>	<b>2</b>
2.1	Device List .....	2
2.2	Viewing the Implantable Device List (IDL) .....	2
2.2.1	Component Menu Bar .....	2
2.2.2	Implant Entry Dialog .....	4
2.3	Adding an Implantable Device to the IDL.....	6
2.3.1	Entering a Known Device (Procedure Documentation) .....	6
2.3.2	Completing the Add Implantable Device Dialog.....	8
2.3.3	Manual Entry or Entering a Historical Device .....	14
2.4	Viewing or Editing Details for an Implanted Device .....	15
2.5	How to Add the IDL Component to the EHR.....	18
2.5.1	Configuring the IDL Component .....	18
2.5.2	Establishing the SNOMED CT Search Function with an NLM Key.....	18
2.6	Incorporating Implantable Device Information from CCDA .....	19
<b>Appendix A</b>	<b>Rules of Behavior .....</b>	<b>20</b>
A.1	All RPMS Users .....	20
A.1.1	Access .....	20
A.1.2	Information Accessibility .....	21
A.1.3	Accountability .....	21
A.1.4	Confidentiality .....	22
A.1.5	Integrity.....	22
A.1.6	System Logon.....	23
A.1.7	Passwords .....	23
A.1.8	Backups.....	24
A.1.9	Reporting.....	24
A.1.10	Session Timeouts .....	24
A.1.11	Hardware .....	24
A.1.12	Awareness.....	25
A.1.13	Remote Access .....	25
A.2	RPMS Developers .....	26
A.3	Privileged Users.....	26
	<b>Acronym List .....</b>	<b>29</b>
	<b>Contact Information .....</b>	<b>30</b>

## Preface

In 2015, the Office of the National Coordinator for Health Information Technology (ONC) published the 2015 Edition Health Information Technology (Health IT) Certification Criteria. In addressing these criteria, Indian Health Service (IHS) has developed the Implantable Device List (IDL) component.

Certified Electronic Health Record (EHR) products are required to offer users a way to record a patient's implanted medical devices, to enter Unique Device Identifiers associated with their devices, parse specific device information and nomenclature from the device identifiers, view a list of such devices, and change the status of implanted devices as needed. This component in the EHR addresses these requirements.

## 1.0 Introduction

Certified EHR products are required to offer users a way to record a patient's implanted medical devices, to enter Unique Device Identifiers associated with their devices, parse specific device information and nomenclature from the device identifiers, view a list of such devices, and change the status of implanted devices, as needed.

Please read all the documentation for EHR v1.1 patch 29 and associated patches. The following documentation is available:

- RPMS Clinical Applications website:  
<https://www.ihs.gov/rpms/applications/clinical/>
- RPMS Trainings/Recordings:  
[https://ihs.cosocloud.com/rpms-tr/event/event\\_info.html](https://ihs.cosocloud.com/rpms-tr/event/event_info.html)

**Note:** If directed to enter a Username and Password, click **OK** to proceed to the Training Repository page.

- RPMS Training Course Materials:  
<https://www.ihs.gov/rpms/training/course-materials/>
- RPMS EHR online help can be located within the RPMS EHR

## 2.0 Implantable Device

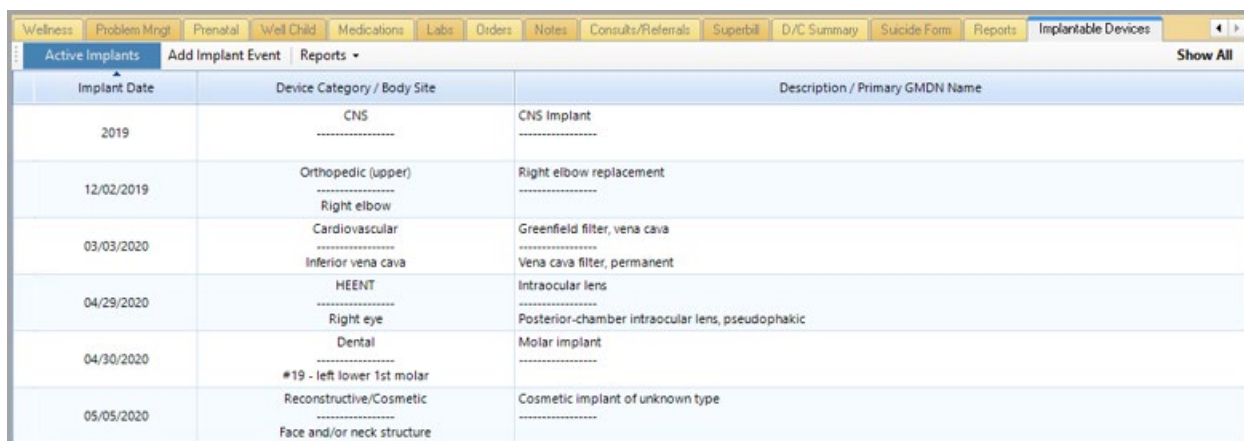
An implantable device is any medical device that may be implanted within the body of a patient, either temporarily or permanently. These devices can range from sutures to artificial joints to cardiac pacemakers. Currently, there are hundreds of thousands, if not millions, of devices documented in various national databases.

### 2.1 Device List

Advances in medicine have made the use of implanted technology frequent, even commonplace, in the treatment of numerous health conditions. The presence of such devices must be taken into consideration in the evaluation of patient symptoms and concerns when ordering diagnostic tests (particularly magnetic resonance imaging or MRI) or planning medical interventions. Moreover, if a device manufacturer should issue a recall, it is helpful to quickly identify patients who are affected. A structured means and location to capture and display this information implantable device is vital.

### 2.2 Viewing the Implantable Device List (IDL)

Each facility determines where the IDL component is located in the RPMS-EHR. The IDL component includes the following features (Figure 2-1).



Implant Date	Device Category / Body Site	Description / Primary GMDN Name
2019	CNS	CNS Implant
12/02/2019	Orthopedic (upper) Right elbow	Right elbow replacement
03/03/2020	Cardiovascular Inferior vena cava	Greenfield filter, vena cava Vena cava filter, permanent
04/29/2020	HEENT Right eye	Intraocular lens Posterior-chamber intraocular lens, pseudophakic
04/30/2020	Dental #19 - left lower 1st molar	Molar implant
05/05/2020	Reconstructive/Cosmetic Face and/or neck structure	Cosmetic implant of unknown type

Figure 2-1: Implantable Device List (IDL) window

#### 2.2.1 Component Menu Bar

The component menu bar includes the following from left to right:

- **Active Implants** – Displays as default. It can be changed to show All Implants (all devices ever entered for the patient) by clicking the **Show All** button on the far right of the title bar and as described below.
- **Add Implant Event** – Used to enter a new Implantable Device.
- **Reports** – Offers a list of two display options.

- **Summary** – Displays a summary table including the following:
  - **Implant Date** – A precise or imprecise date of the implant.
  - **Status** – Active or Inactive implant status. If the device is Inactive, a reason follows in parenthesis including (E) entered in error, (X) expired, or (R) removed.
  - **Category** – Implantable device category by general body location.
  - **Description** – Description of the implantable device.
  - **Detailed** – Displays a list of all implantable devices with Implant Date, Category, Body Location, Facility, Status, Description, Associated Problems, Comments, and detailed device information (if available) that was scanned or manually entered.
- **Show All** – Click this text button to toggle the view between **Active Implants** and **All Implants** as described above. Select this to view all devices ever entered for the patient, not just the active devices (default). The text switches from bold font to normal font when changing between views.

**Note:** The **Show All** view defaults to bold font and shows only Active Implants each time the EHR is launched.

- Display Columns – Sortable with a toggle between ascending or descending by clicking the column header bar.
- Implantable Device Rows – There is one row for each Implantable Device recorded for the patient. Each row includes:
  - **Implant Date** – This may be an imprecise date if the exact date of implantation is unknown.
  - **Device Category/Body Site**
    - There are 10 Device Categories that may be recorded.
    - Body Site is the specific location (body part) of the implanted device if this has been recorded.
  - **Description/Primary GMDN Name** – There are two descriptions of the implanted device, one or both of which may be present.
    - Implant description is a free-text field entered manually.
    - **Primary GMDN Name** is a description of the device from the Global Medical Device Nomenclature (GMDN) database, a list of generic names used to identify all medical device products.

## 2.2.2 Implant Entry Dialog

In the process of either adding an implant event or viewing/editing an implant, the **Implant Entry** dialog displays. The title bar for the window displays **Add Implant for <patient>** or **View/Edit Implantable Device**, as in Figure 2-2, depending on how the window was accessed.

The procedures for accessing and populating the data in this dialog are described in Section 2.3. The following is a list and general description of the elements captured in this entry dialog.

Figure 2-2: View/Edit Implantable Device dialog

The dialog contains the following information, if known or previously entered.

### Upper Portion of Dialog

- **Device Category** – A menu of 10 categories, such as Cardiovascular, CNS, General Surgical, HEENT, Orthopedic (upper), Orthopedic (lower), etc.

**Note:** This is the only field in this dialog that *cannot* be modified after the initial entry is saved.

- **Implant Description** – A free-text field to describe the implantable device in clinically relevant terms.

**Note:** The **Implant Description** is a required field. For some implants recorded historically, this will be the only description of the implant that will be available.

- **Implant Location** (optional) – A list of possible body locations for the implanted device based upon the chosen Device Category.
- **Implanted Date** – May be precise or imprecise, as available.
- **Implanted at (facility)** – Searchable list or free-text entry of facility location.
- **Implanter** – Searchable list or free-text entry of the performing provider.
- **Associated Problem** – A list of Active Problems from the Integrated Problem List (IPL).
- **Procedure Code** – A procedure code lookup for the implanted device.
- **Comments** – A field for entering general comments which can be amended at any time with a date/time stamp on each comment addition.

### Lower Portion of Dialog

This is separated from the upper portion by a menu bar with **Add a Device** and **Remove a Device** buttons and a check box to manually edit information in the device fields.

In some cases, a single procedure may result in implantation of multiple devices. An orthopedic fracture repair, for example, might include a plate and screws. A joint replacement might include separate parts for the ball and socket. Therefore, this lower portion may contain a single device or multiple devices within the same dialog as denoted by individual tabs for each device with the following details:

- **Product Identifier** – Alphanumeric string from product packaging.
- **SNOMED CT Description**
- **GMDN Name** – The Global Medical Device Nomenclature (GMDN) is a list of generic names used to identify all medical device products.



- **Manufacturer / Company**
- **Product Brand Name**
- **Product Description**
- **Version or Model**
- **Serial Number**
- **Lot/Batch Number**
- **Manufacture Date**
- **Expiration Date**
- **MRI Safety Information**
- **Contains Natural Rubber or Latex when Checked** check box
- **HCT/P** check box – This is a unique code required for any implant comprised of human cellular or tissue products.

If changes have been made in the **View/Edit Device** dialog, the **Save Changes** button is enabled. Click **Save Changes** to exit or **Cancel** to exit without saving.

## 2.3 Adding an Implantable Device to the IDL

There are two typical scenarios for adding an Implantable Device to the IDL:

- The patient has undergone a procedure at your facility, and the device is being documented as part of that procedure.
- While documenting patient history, it is learned that the patient has an implanted device. It is important to add to the patient record.

Facilities must determine by policy which types of devices should be recorded in the EHR. For example, a facility may determine that resorbable sutures or dental implants do not need to be recorded, but contraceptive implants, intrauterine devices, or coronary artery stents should be documented.

A site may also determine that all devices from a specific procedure, such as screws and pins, do not need to be documented in detail, but the principal device, such as an artificial joint, should be documented.

### 2.3.1 Entering a Known Device (Procedure Documentation)

The ideal time to document an Implantable Device is at the time of (or immediately following) a procedure before any packaging accompanying the device has been discarded.

1. Open the RPMS-EHR.
2. Select the Patient.

3. Select the **Encounter Context**.

**Note:** This is not required, but users cannot enter a Procedure code if the Encounter Context is not set.

4. Navigate to the IDL component.
5. Click the **Add Implant Event** button to display the **Add Implantable Device** (Figure 2-3).

The screenshot shows a modal dialog titled "Add Implant for Demo, Patient". The dialog is divided into several sections. At the top, there is a dropdown menu for "Device Category\*" and a text input field for "Implant Description\*" with a placeholder "(Free text, up to 75 characters)". Below these are "Implant Location (optional)" and "Implanted Date\*" dropdowns. To the right, there are three search fields: "Implanted at (facility)" with the value "2017 DEMO CLINIC CHIT", "Enter person implanting device", and "Enter procedure code" with the value "Procedure - CPT/ICD-10 PC". Below the search fields is an "Implanter" field. At the bottom left, there is a large text area for "Comments" and an "Add Comment" button. At the bottom right, there are "Save" and "Cancel" buttons. The dialog also features "Add a Device" and "Remove a Device" buttons at the bottom center.

Figure 2-3: Add Implant Device dialog

**Note:** This is a *modal* dialog, meaning it must be completed or closed before navigating elsewhere in the EHR.

## 2.3.2 Completing the Add Implantable Device Dialog

To complete adding the implantable device, follow the steps below:

1. Complete the upper portion of the dialog by entering the following information.

**Note:** The **Device Category**, **Implant Description**, and **Implanted Date** fields are mandatory to complete the implant entry.

- **Device Category** – Select this required category from the options.
- **Implant Description** – This is a required, free-text field used to describe the implantable device in clinically relevant terms.
- **Implant Location** – Specify where in the body the implant is located. This is a list of possible body locations for the implanted device based upon the chosen Device Category. If the body part is not on the list, select **Other**. An additional dialog opens for a search of more body locations (Figure 2-4).

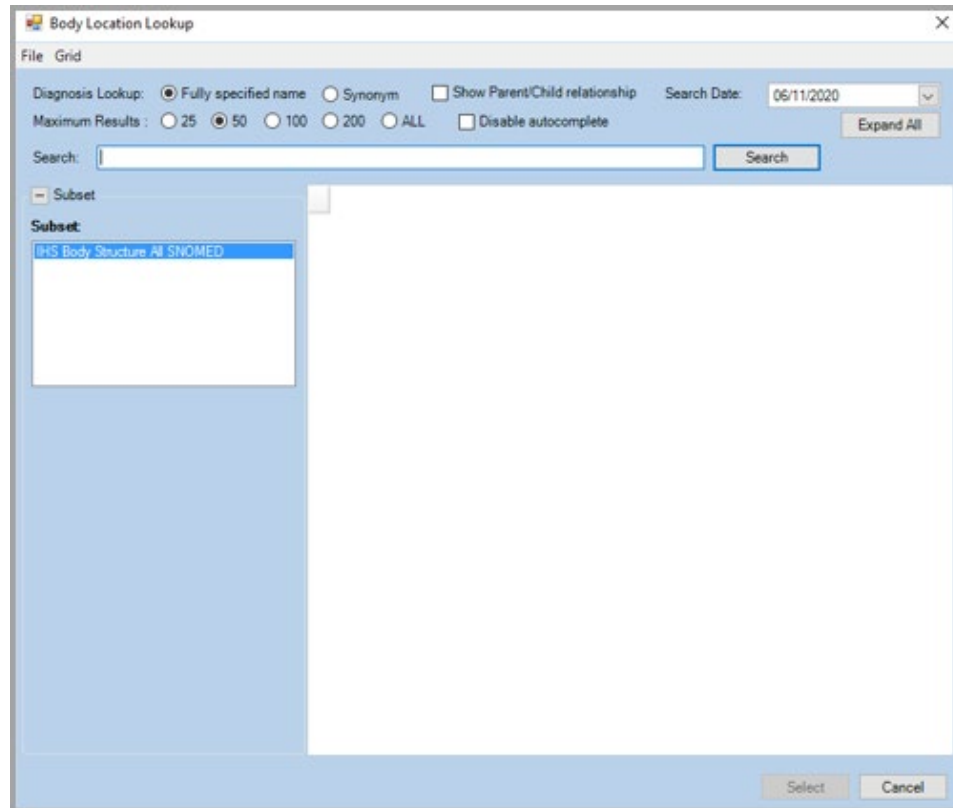


Figure 2-4: Body Location Lookup dialog

- Enter the body location in the **Search** field and click **Search** to displays a list of body locations. Double-click the body location to populate the **Implant Location** field and return to the **Add Implant** dialog.

- **Implanted Date** – Enter the date of the implant as an exact date or as an imprecise date (t-days, or month/year or year only) if the exact date of implant is not known.
- **Implanted at (Facility)** – Defaults to the current facility. A different facility may be entered using the search function (magnifying glass icon) within the dialog (Figure 2-5).

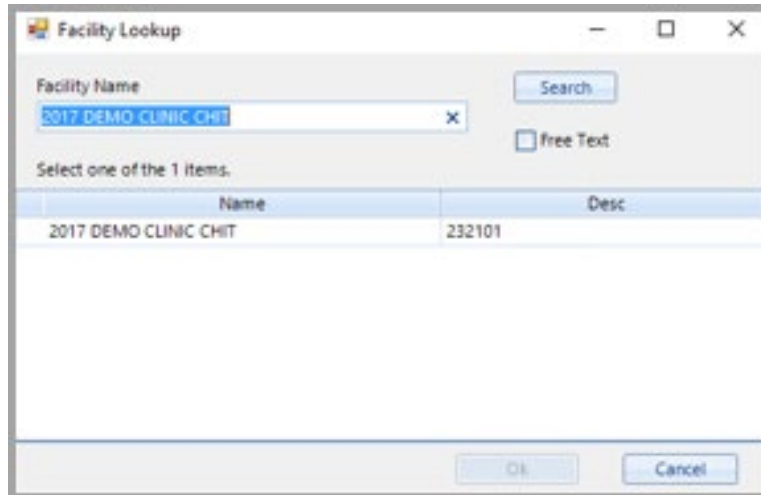


Figure 2-5: Facility Lookup dialog

- The user can also select the **Free Text** check box (Figure 2-6). This allows the user to click the **Unknown** button if the Facility name is not available, and the word Unknown will populate the **Facility Name** field.



Figure 2-6: Facility Lookup dialog – Free Text check box selected

- **Implanter** – Defaults to the current provider if the device is being entered in the context of a visit. A different implanter may be entered using the search function (magnifying glass icon) within the dialog (Figure 2-7). Users can also select the **Free Text** check box. This allows the user to click the **Unknown** button if the Implanter name is not available, and the word Unknown will populate the **Implanter** field.

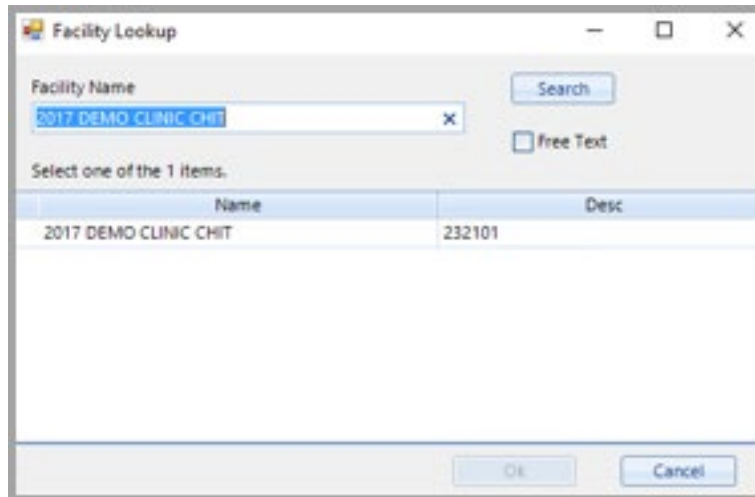


Figure 2-7: Implanter Lookup dialog

- **Associated Problem** – A list of active problems from the Integrated Problem List (IPL). If the cause for which the implanted device procedure was done is available, it can be selected here, or the entry can be left blank.

**Note:** Users cannot add a new problem from this dialog. This must be completed on the IPL.

- **Procedure Code** – If the encounter context is set, users can enter a CPT or ICD-10 PC code for the device implantation procedure (Figure 2-8). Click the search button (the magnifying glass icon) on the **Enter procedure code** entry:

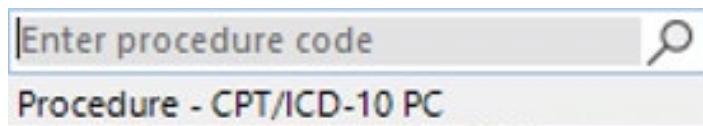


Figure 2-8: Enter procedure code search field

This the **Procedure Lookup** dialog (Figure 2-9) displays, where the user can search the Lexicon, CPT, or ICD code sets.

Figure 2-9: Procedure Lookup dialog

- Each facility has a list of procedure codes approved by its billing staff for implantable device procedures performed at the site. Refer to this list when entering the procedure code.

Only enter procedure codes for procedures completed during this encounter.

**Note:** Procedure codes entered in this dialog will not populate the procedure fields in other areas of the EHR.

- **Comments** – The user can enter a brief comment to supply additional information about the implantable device or procedure. This is not a procedure note, which should be documented using the appropriate note title in the Text Integration Utilities (TIU) component of EHR.
    - Once saved, comments cannot be edited, but new comments may be added.
    - Each comment will have a date/time stamp associated with it.
    - Any future changes to the device information will also tracked in this field with a date/time stamp and the following comment: “This record has been updated.”
2. Click the **Add a Device** button to open the device detail fields in the lower portion of the dialog.
  3. Place the cursor in the **Product Identifier** control (Figure 2-10).

Figure 2-10: Add Implant for &lt;patient&gt; dialog

4. Using a connected bar-code scanner, scan the bar code from the implant device packaging. The barcode may be labeled with terms such as **Device Identifier**, **Production Identifier**, and/or **Unique Device Identifier**.
  - If there is more than one bar code, scan them sequentially, in the order they appear on the product label. Click the **Add a Device** button and place the cursor in the **Product Identifier** control before scanning each bar code.

**Warning:** Always scan the bar code from the device's original packaging to ensure the unique information is captured including the serial number, lot number, manufacturer, and expiration dates.

- If a bar-code scanner is not available, enter the alphanumeric string from the bar codes on the packaging. These strings can be lengthy, so it is important to double-check for accuracy.
  - If no packaging is available, enter as much information about the device as possible, as described in Section 2.3.3.
  - The **Remove a Device** option may be used to delete a device entered in the lower field in error.
5. Click the **Search** button once the code is entered and checked.
- If the search is successful, the shaded fields in the **Add a Device** dialog populate with information from the national Implantable Device Database.
  - In addition, the device tab located beneath the **Add a Device** button will change from **Unknown** to the product brand name for the device.

Figure 2-11: Add a Device dialog

- If the search is not successful, a pop-up dialog displays the message: **“Specified Product was not found.”**

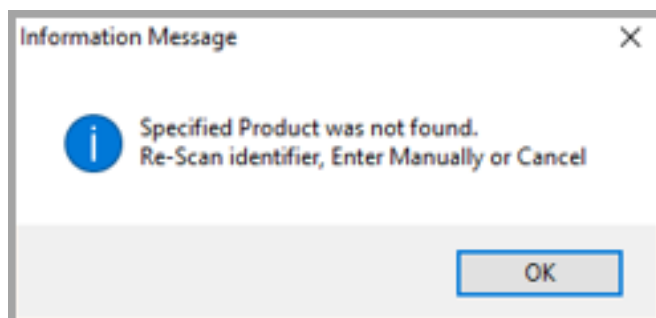


Figure 2-12: Specified product not found message



If this occurs:

- a. Click **OK** on the pop-up dialog.
- b. Clear the **Product Identifier** control and re-scan (or manually enter) the code.
- c. Click **Search**.

If the search fails again, see Section 2.3.3 for manual entry.

6. Close the dialog. If changes have been made in the **Add Implantable Device** dialog, the **Save** button is enabled.
7. Click **Save** to exit or **Cancel** to exit without saving.

### 2.3.3 Manual Entry or Entering a Historical Device

To document an implantable device based on the patient's history, if the device packaging is not available, or if the scan/search method described above is not working, the device information can be entered manually.

**Note:** Many manufacturers, especially those of particularly risky or invasive devices, provide the patient with a document (wallet card) that includes much of the information. Enter the device details from the patient's wallet card if possible.

1. Click the **Add Implant Event** button to open the **Add Implant** dialog.
2. Complete the upper portion of the dialog by completing the mandatory fields of **Device Category**, **Implant Description**, and **Implanted Date**. The following fields may be completed if the information is available:
  - **Implant Location**
  - **Implanted At** (facility)
  - **Implanter**
  - **Associated Problem**
  - **Procedure code**, if documenting a current procedure at your facility

**Note:** Do not enter a procedure code on a historical device entry.

- **Comments**
3. Click the **Add a Device** button to open the **Device Detail** fields in the lower portion of the dialog.
  4. Select the **Checked if device info was manually entered** check box. This un.masks fields normally retrieved by electronic searching, allowing manual entry.

Figure 2-13: Dialog to Add a Device or Remove a Device

5. Complete as many of the fields as possible about the implanted device based on the patient's history, wallet card, or product packaging.
6. Use the **Add a Device** button to add any additional devices or components, if available, for a single implant event entry. The **Remove a Device** button may be used to delete a device entered in the lower field in error.
7. Close the dialog. If changes have been made in the **Add Implantable Device** dialog, the **Save** button is enabled.
8. Click **Save** to exit or **Cancel** to exit without saving.

## 2.4 Viewing or Editing Details for an Implanted Device

In most cases, the initial display of implanted devices offered in the IDL component should be sufficient for review. However, if details about any device are needed, or if the implant details need to be modified in any way, this may be performed in the following ways:

1. Right-click the device to display a context menu (Figure 2-14) with the following options:

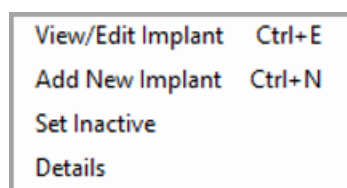


Figure 2-14: Implanted Device context menu

- **View/Edit Implant** – Opens the **View/Edit Implantable Device** dialog with the instructions as described below.
- **Add New Implant** – Opens a dialog to add a new implant event with instructions as described in Section 2.3.
- **Set Inactive** – Opens a sub-menu dialog (Figure 2-15) with the following options to inactivate a device from the list:

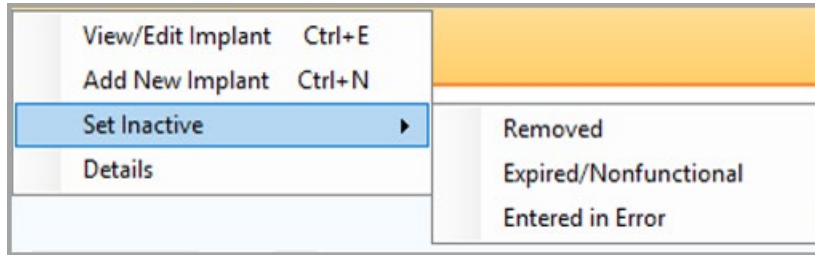


Figure 2-15: Set Inactive Options dialog

- **Removed** – The device has been removed from the patient. This is represented as Inactive (R) in the summary report.
  - **Expired/Nonfunctional** – The device has reached the end of its lifespan or has been determined to be ineffective but remains in the patient’s body. This is represented as Inactive (X) in the summary report.
  - **Entered in Error** – The Implantable Device entry has been determined to be erroneous (for example, including incorrect device information or entered in the wrong patient’s record). This is represented as Inactive (E) in the summary report.
- **Details** – Displays the details of the individual implant event including the Implant Date, Category, Body Location, Facility, Status, Description, Associated Problem, Comments, and the more detailed device information (if available) that was scanned or manually entered.
2. Double-click the device to display the **View/Edit Implantable Device** dialog (Figure 2-16). This is the same dialog that is accessed by right-clicking the device and selecting **View/Edit Implant**, as described above.

Figure 2-16: View/Edit Implantable Device dialog

**Note:** This is a *modal* dialog, meaning it must be completed or closed before navigating elsewhere in the EHR.

3. The user can navigate through the fields and make changes, as necessary. All fields are modifiable with the exception of the **Device Category**, which is a fixed field after the implant was saved the first time.
4. If changes have been made in the **View/Edit Device** dialog, the **Save Changes** button is enabled. Click **Save Changes** to exit or **Cancel** to exit without saving.

## 2.5 How to Add the IDL Component to the EHR

The IDL component may be added to the EHR design template by users with Design Mode privileges. Typically, this is a Clinical Applications Coordinator, an Informaticist, an IT Specialist, or an RPMS Site Manager.

A suggested location for the IDL, for example, would be on a tab next to the Integrated Problem List (IPL), making it easy for users to navigate to the IDL from the IPL.

### 2.5.1 Configuring the IDL Component

The IDL Component is issued as a nationally standardized component of the EHR. No local configurations are supported.

### 2.5.2 Establishing the SNOMED CT Search Function with an NLM Key

Each implantable device has a GMDN description and a SNOMED CT description. In most cases, these two descriptions are identical. Although only the GMDN description displays in the IDL user interface. Both terms are included in the CCDA extract from RPMS that includes the list of implanted devices. Retrieving the SNOMED CT description requires an additional setup step as described below.

The SNOMED CT description for an implanted device is retrieved when the EHR sends an application programmer interface (API) key to the National Library of Medicine (NLM). This occurs in the background, but the key is granted by the NLM to a named user at the site who must register with the NLM. Then, the NLM Key is obtained by establishing a free account with the Unified Medical Language System (UMLS). This account must be renewed yearly, and account holders typically receive a notification one month before the account expires.

One person (“account holder”) from each site should register on the UMLS Terminology Services website: <https://uts.nlm.nih.gov/home.html>.

- Account holders can be a CAC, administrator, or any person at the facility.
  - Account holders create a free account with identifiers, a username, and a password.
  - Account holders will receive an email to verify the email address.
  - Once verified, the account will be created typically within days.
1. Locate the UMLS API Key in the account holder’s profile.
    - a. Go to the above link and log in to the account.
    - b. Click **My Profile** at the top.
    - c. The UMLS API Key is part of the profile.

2. Enter the UMLS API Key into the EHR to enable the SNOMED CT search.
  - a. To enter, use the normal XPAR menu options.
  - b. The value can be set at the System and User levels for all users.
  - c. BEHOIMP UMLS API KEY general parameter.

## 2.6 Incorporating Implantable Device Information from CCDA

Clinical summary documents that follow the Consolidated Clinical Document Architecture (CCDA) standard version 2.1 or later may include data on Implantable Devices.

Future versions of the RPMS-EHR Clinical Information Reconciliation (CIR) component will include the ability for users to directly incorporate this information from summary documents into the EHR. This data will then appear in the Implantable Device List and will be exported with the CCDA summary document.

## 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.cfm>.

<p><b>Note:</b> Users must be logged on to the IHS D1 Intranet to access these documents.</p>
---

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 ROB 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.

## Acronym List

Acronym	Meaning
API	Application Programmer Interface
CCDA	Consolidated Clinical Document Architecture
CIR	Clinical Information Reconciliation
CIR	Clinical Information Reconciliation
EHR	Electronic Health Record
GMDN	Global Medical Device Nomenclature
HHS	United States Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
IDL	Implantable Device List
IHS	Indian Health Service
IPL	Integrated Problem List
ISSO	Information System Security Officer
MRI	Magnetic Resonance Imaging
NLM	National Library of Medicine
ONC	Office of the National Coordinator for Health Information Technology
RPMS	Resource and Patient Management System
SAC	IHS RPMS Programming Standards and Conventions
TIU	Text Integration Utilities
UMLS	Unified Medical Language System



## 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](mailto:itsupport@ihs.gov)