RESOURCE AND PATIENT MANAGEMENT SYSTEM

Personal Health Record

(BPHR)

Web Portal Administrator Manual

Version 2.0 Patch 5
September 2020

Office of Information Technology
Division of Information Technology

Table of Contents

Preface

This administrator manual provides instructions for using the Indian Health Service (IHS) Personal Health Record (PHR) Administrator Web Portal –Version 2.0 application.

The contents of the PHR Administrator Manual are organized by subject matter, with headings and pages corresponding to the PHR Administrator Web Portal menus and options. All images shown herein contain no real data and are used for illustration purposes only.

> **Note:** To avoid redundancy, this user manual does not include background information on such topics as the Resource and Patient Management (RPMS) system, the IHS Master Patient Index (MPI), the IHS Health Information Exchange (HIE), or a summary of changes in this version of the application.

Revision History

Version	Date	Description	Sections
1.0	10/1/2015	Initial Release	All
1.1	12/15/2016	v2.0 Patch 1 Updates	4.3, 4.4, 9.0
1.2	02/10/2017	v2.0 Patch 2 Updates	3.0 through 11.0
1.4	12/1/2017	V2.0 Patch 3 Updates	6.3, 7.0, 7.1
1.5	11/15/2018	V2.0 Patch 4 Updates	2.9, 6.0 through 10.4
1.6	8/24/2020	V2.0 Patch 5 Updates	Entire document. Updated images and procedures and proofread

1.0   Introduction

This manual is intended for all IHS administrators of the PHR, including the National PHR Administrator, Area Office (AO) Administrators, Service Unit/Facility Administrators (SU/FA), and PHR Registrars. The PHR Administrator Web Portal application lets administrators perform the responsibilities based on their role (see Section 1.4). These responsibilities include creating administrator accounts, managing patients, creating reports, managing accounts, processing PHR access applications, and updating user profiles.

This manual in its entirety can be accessed from the PHR Administrator Web Portal application Help link at https://phradmin.ihs.gov/phr-admin-web/login.

1.1   PHR Background

The IHS Office of Information Technology (OIT) developed the PHR to help IHS patients manage their health more effectively. The PHR is a secure and private internet application that conforms to all federal privacy laws and regulations. It enables verified patients, and their authorized representatives, to view their clinical information. This health information includes allergies, medications, health issues, recent lab results, immunizations, recent vital signs, implantable devices, and procedures in electronic form. By using the PHR to access health information between visits, patients can:

- Ensure the information in their medical record is correct.

- Learn more about their medications and health issues.

- Save, print, and email a copy of their health information.

- Share their health information with a caregiver or other personal representative.

- Prepare questions or concerns they would like to discuss with their health care providers.

- Exchange messages with their health care team using a private and secure email system.

Patients can share their health information with their personal representatives. Patients who have completed the verification process can delegate, manage, and revoke access to their PHR for any registered PHR user. A registered PHR user is someone who has registered to use the IHS PHR and may or may not have completed the verification process. The verified PHR user delegating access can manage the areas of their PHR that the delegate can and cannot view through access controls.

> **Note:** The PHR will suppress specific health-related information for an un-emancipated minor (Minor) PHR user, such as family planning, contraceptives, and pregnancy. Parent, guardian, or individual acting in *loco parentis* that have been granted delegate access to the Minor's PHR will be revoked automatically when the Minor reaches the age of majority (18th birthday). If the Minor becomes emancipated, the PHR Registrar will revoke delegation access as part of the operational process and update their emancipated minor status (see Section 10.4). The patient will have to reestablish their PHR through the verification process to access their PHR (see Section 6.0).

1.2   PHR Administrator Web Portal Application Requirements

The PHR Administrator Web Portal is a stand-alone web application in which PHR Administrators and Registrars may have limited access to Protected Health Information (PHI)/ Personally Identifiable Information (PII). Therefore, all computers used for the PHR Administrator Web Portal application must be used on computers where the environment is secure, its hard drive and storage media is encrypted, and other storage media is encrypted.

The PHR Administrator Web Portal supports the latest versions of the following Internet browsers:

- Microsoft Internet Explorer

- Microsoft Edge

- Google Chrome

- Firefox

> **Note:** Although Internet Explorer is supported, Microsoft security patches may cause some functionality to perform inconsistently. If you experience an issue with the Internet Explorer browser, try using one of the other supported browsers. You may need to contact the IT department to install the latest version of Google Chrome or Firefox.

1.3   PHR Administrative Access Requirements

Each authorized PHR administrator must complete the following steps to gain access to the PHR Administrator Web Portal application. Access request method may vary based on Service Unit/Facility's local policy and procedure; however, the registration process for all authorized PHR administrators must include an in-person identity verification. Upon identity verification, PHR administrators will need to complete the process based on the administrative role in Section 1.4. Each PHR Administrator must comply with the auditing policies outlined in the PHR Audit Policy and the Health Insurance Portability and Accountability Act (Chapter 7 - Health Insurance Portability and Accountability Act Privacy Rule and the Privacy Act).

> **Note:**   Unauthorized use of the PHR Administrator Web Portal application is not covered by the Privacy Act of 1974 Section 522a.

1.4   PHR Administrator Roles and Responsibilities

The PHR Administrator Web Portal application consists of four administrator roles: National Administrator, AO Administrator, Service Unit/Facility (SU/FA) Administrator, and the PHR Registrar.

1.4.1   National Administrator Role

The PHR system limits the number of National Administrators to three (3), which are appointed by the IHS Chief Information Officer. This role is limited to individuals who are IHS employees or their designee who have National Security responsibilities. National Administrators will need to complete the following to gain access to the PHR Administrator Web Portal application:

- Complete in-person identity verification.

- Upon identity verification, the PHR project Federal Lead will complete the Information Technology Access Control (ITAC) system to request and track access for National Administrators.

- Once the ITAC has been approved, the Federal Lead or designee will create the National Administrator account.

- The PHR Federal Lead will also coordinate access and training for the PHR Administrator Web Portal application.

National Administrators possess the following privileges:

- Create, read, update, or delete (CRUD) other National Administrator accounts.

- CRUD AO Administrator accounts.

- Read SU/FA and PHR Registrar accounts.

- Unlink or inactivate PHR User access

- Generate audit reports for every user of the PHR, which includes users of the PHR Administrator Web Portal and PHR Patient Web Portal applications.

The National Administrator responsibilities include the following:

- Verify the identity of other National Administrators and AO Administrators.

- Create PHR Administrator Web Portal accounts for other National Administrators and AO Administrators.

- Update/Change other National Administrator and AO Administrator passwords upon request.

- Update, inactivate, or reactivate other National Administrators' and AO Administrators' account information.

- Provide PHR Administrator and Patient Web Portal training to AO Administrators.

Additional responsibilities may include the following as an AO Administrator, SU/FA Administrator, or PHR Registrar backup.

- Update/Change PHR User password upon request.

- Unlink or inactivate PHR Users from their IHS Medical Record.

- Respond to other PHR User help requests.

1.4.2   AO Administrator Role

The PHR system limits the number of AO Administrators to ten (10), which are appointed by the Area Information System Security Officer (ISSO) or supervisor for each AO. AO Administrators will need to complete the following to gain access to the PHR Administrator Web Portal application:

1. Upon identity verification, the Area ISSO or supervisor will complete the ITAC system to request and track access for AO Administrators.

2. Once the ITAC has been approved, the National Administrator will create the AO Administrator account.

3. The PHR Federal Lead or National Administrator will coordinate access and training for the PHR Administrator Web Portal application.

> **Note:** For facilities that do not buy Area shares, the National Administrator will create an independent Area for each of these facilities. These facilities will assume the responsibilities of this role in addition to any facility defined roles.

AO Administrators possess the following privileges:

- Read other AO Administrator accounts within the administrator's AO.
- CRUD SU/FA Administrator and PHR Registrar accounts for a facility within the administrator's AO.
- Unlink or inactivate PHR User access.
- Generate audit reports to monitor system level activities for their Area Service Units and facilities.
- Reset own password.

The AO Administrator responsibilities include the following:

- Verify the identity of the SU/FA Administrator.
- Create PHR Administrator Web Portal accounts for SU/FA Administrators.
- Update/Change SU/FA Administrator passwords upon request.
- Update, inactivate, or reactivate SU/FA Administrators account information.
- Provide PHR Administrator and Patient Web Portal training to the SU/FA Administrator.
- Perform as a back-up SU/FA, if needed.

Additional responsibilities may include the following as a SU/FA Administrator or PHR Registrar backup.

- Verify the identity of the PHR Registrar for the SU/FA.
- Create PHR Administrator Web Portal accounts for the SU/FA PHR Registrar.
- Update/Change SU/FA PHR Registrar password upon request
- Update, inactivate, or reactivate SU/FA PHR Registrar account information.
- Update/Change PHR User passwords upon request.
- Unlink or inactivate PHR Users from their IHS Medical Record.
- Respond to other PHR User help requests.

1.4.3   Service Unit/Facility Administrator Role

The PHR system limits the number of SU/FA Administrators to six (6) per each Service Unit/Facility, which are appointed by the Indian, Tribal, or Urban Chief Executive Officer or local Health Information Management (HIM) staff. SU/FA Administrators will need to complete the following to gain access to the PHR Administrator Web Portal application:

1. Facilities on the IHS D1/Active Directory will complete the ITAC system to request access for their SU/FA, while Tribal and Urban facilities not on the IHS D1/Active Directory will need to open an OIT Headquarters helpdesk ticket at ITsupport@ihs.gov for their designated AO Administrator to request and track access for SU/FA Administrators.

2. Once the ITAC or helpdesk ticket has been approved, the AO Administrator will create the SU/FA Administrator account.

3. The PHR Federal Lead or AO Administrator will coordinate access and training for the PHR Administrator Web Portal application.

SU/FA Administrators may be responsible for more than one service unit or facility and possess the following privileges:

- Read other Service Unit/Facility Administrator accounts within the administrator's own Service Unit/Facility.

- CRUD PHR Registrar accounts within the administrator's Service Unit/Facility.

- Unlink or inactivate PHR User access.

- Generate audit reports to monitor local facility system activities.

The SU/FA Administrator responsibilities include the following:

- Verify the identity of the SU/FA PHR Registrars.

- Create PHR Administrator Web Portal accounts for SU/FA PHR Registrars.

- Update/Change PHR Registrars password upon request.

- Update, inactivate, or reactivate PHR Registrar account information.

- Prepare SU/FA specific PHR Administrator and Patient Web Portal training materials for the SU/FA PHR Registrar.

- Provide PHR Administrator and Patient Web Portal training to the SU/FA PHR Registrar.

- Inform Patient Registration Clerks to ask patients if they have PHR Access.

- Conduct regular audits.

Additional responsibilities as a PHR Registrar backup may include the:

- Update/Change PHR User passwords upon request.

- Unlink or inactivate PHR Users from their IHS Medical Record.

- Respond to other PHR User help requests.

- May need to update RPMS PHR Access field.

1.4.4   PHR Registrar Role

The PHR system does not limit the number of PHR Registrars that a facility can create; however, facilities should limit the number of PHR Registrars based on demand and the facilities' policies and procedures. Service units and facilities will determine the job function that will fill this role. The IHS HIM Consultants Committee recommends that service units and facilities consider HIM and Patient Registration Clerks to fill the PHR Registrar role. PHR Registrars will need to complete the following to gain access to the PHR Administrator Web Portal application:

1. Facilities on the IHS D1/Active Directory will complete the ITAC system to request access for their SU/FA, while Tribal and Urban facilities not on the IHS D1/Active Directory will need to open an OIT Headquarter helpdesk ticket at ITsupport@ihs.gov for their designated SU/FA Administrator to request and track access for PHR Registrars.

2. Once the ITAC or helpdesk ticket has been approved, the SU/FA Administrator will create the PHR Registrar account.

3. The PHR Federal Lead or SU/FA Administrator will coordinate access and training for the PHR Administrator Web Portal application.

The PHR Registrar possesses the following privileges:

- Update/Change own password.

- Process PHR access applications

- Read patient profile information.

- Generate PHR user-requested audit reports.

> **Note:** PHR users are users who have registered to use the PHR. This role is defined in the Personal Health Record User Manual.

The PHR Registrar responsibilities include the following:

- Verify registered PHR User's (patient) identity.

- Process PHR applications, which include matching and linking patient records with their IHS Medical Record.

- Process request PHR access for minors.

- Process the IHS-810 form according to the Service Unit/Facility's policies and procedures.
- Register and process the minor's PHR account access, as described in Section 6.0, once the minor's request for access IHS-810 form is approved, if necessary.

> **Note:** The PHR Registrar will need to record the minor's PHR Username, Password, and Security Questions and Answers on the IHS-810 form and file the form according to the Service Unit/Facility's policies and procedures.

- Grant the minor's parent, legal guardian, or court appointed guardian access to the minor's PHR as described in Section 10.0

- Process the request for PHR access for the legal guardian of an elderly patient or a patient living with mental illness.

- Process IHS-810 form according to the Service Unit/Facility's policies and procedures.
- Register and process the patient's PHR account access, as described in Section 6.0, once the patient's request for access IHS-810 form is approved, if necessary.

> **Note:** The PHR Registrar must record the patient's PHR Username, Password, and Security Questions and Answers on the IHS-810 form and file the form according to the Service Unit/Facility's policies and procedures.

- Grant the legal guardian access to the patient's PHR as described in Section 10.0.

- Update/Change PHR User passwords upon request.

- Unlink or inactivate PHR Users from their IHS Medical Record.

- Verify patient access can access their PHR.

- Prepare SU/FA specific PHR training materials.

- Review PHR training materials with registered PHR users.

- Respond to PHR User help requests.

2.0   PHR Administrator Web Portal Common Functions

The PHR Administrator Web Portal provides administrators with common functionality on each page throughout the portal.

2.1   Logon

The PHR Administrator Web Portal application is located at https://phradmin.ihs.gov (Figure 2-1). This page allows PHR administrators to view information about the PHR, the privacy policy, terms and conditions, contact information, PHR Administrator Manual (Help), and to logon to the PHR Administrator Web Portal application. Only PHR administrators (National, Area, SU/FA, and PHR Registrars) who have completed the access requirements in Section 1.2 and received a PHR administrator username and password can logon to the portal.

Figure 2-1: PHR Administrator Web Portal Application Login

To logon to the PHR Administrator Web Portal application:

1.   Go to https://phradmin.ihs.gov (Figure 2-1).

2. Enter your administrator **Username**.

3. Enter your **Password**.

4. Click **Login**. The PHR will redirect the administrator to the **Welcome** page (Figure 2-2). Access administrator privileges from the **Welcome** page.

> **Note:** If this is the first time the administrator logs into the PHR Administrator Web Portal Application or the administrator had their password reset by an up-level PHR Administrator, the administrator will be prompted to reset their password. (see Section 5.0 for more information.)

Figure 2-2: Welcome page for National Administrators, AO Administrators, and SU/FA Administrators
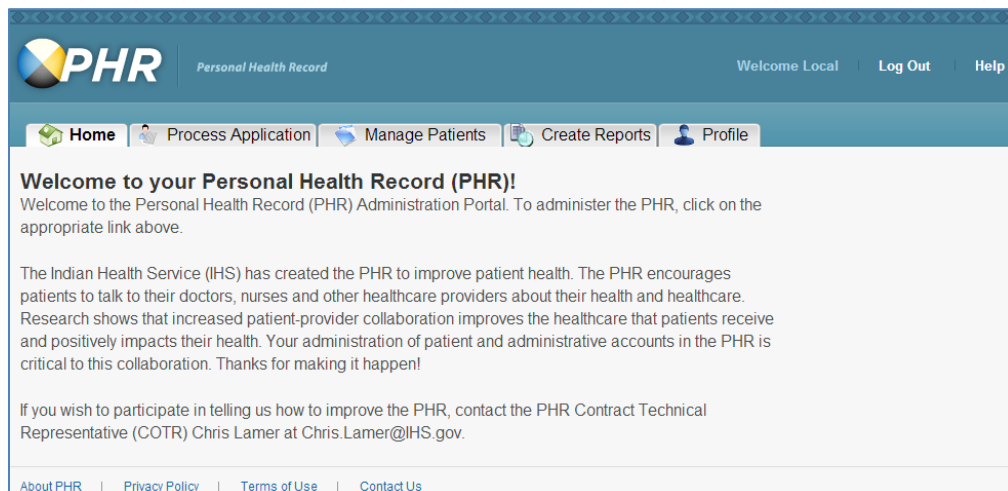

Figure 2-3: Welcome page for PHR Registrar Administrators

2.2   Help

To access the PHR Administrator Web Portal manual, click **Help** in the upper right corner of the page (Figure 2-2 and Figure 2-3).

2.3   Search Results

1.   Click on the **Manage Account** tab.

Figure 2-4: Manage Account tab, Search for Administrative Account

2.   Enter criteria into the appropriate fields and click **Search**.

> **Note:**   The asterisk (*) symbol can be used as a wildcard to replace zero or more characters in a word. For example, to search for accounts with a last name that begins with "Demo," type **Demo*** in the **Last Name** field. The search results will display every administrator user with the selected role that begins with Demo, such as Demo, Demos, Demotest, Demouser, demoprovider, etc.

2.4   Sorting Search Results

Search Results from the **Manage Account** (Figure 2-5)**, Process Application**, **Manage Patients**, or **Create Reports** tabs can be sorted or modified. The procedure is the same for each.
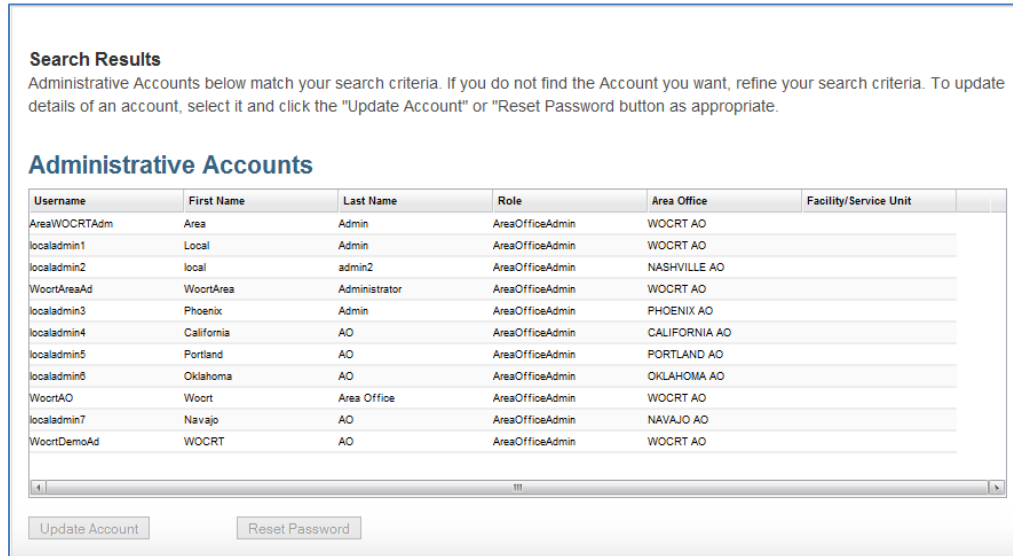

Figure 2-5: Search Results page for Administrative Accounts tab

1. Click the column header of the returned table (Figure 2-5) to sort the table by that column in ascending order (Figure 2-6).

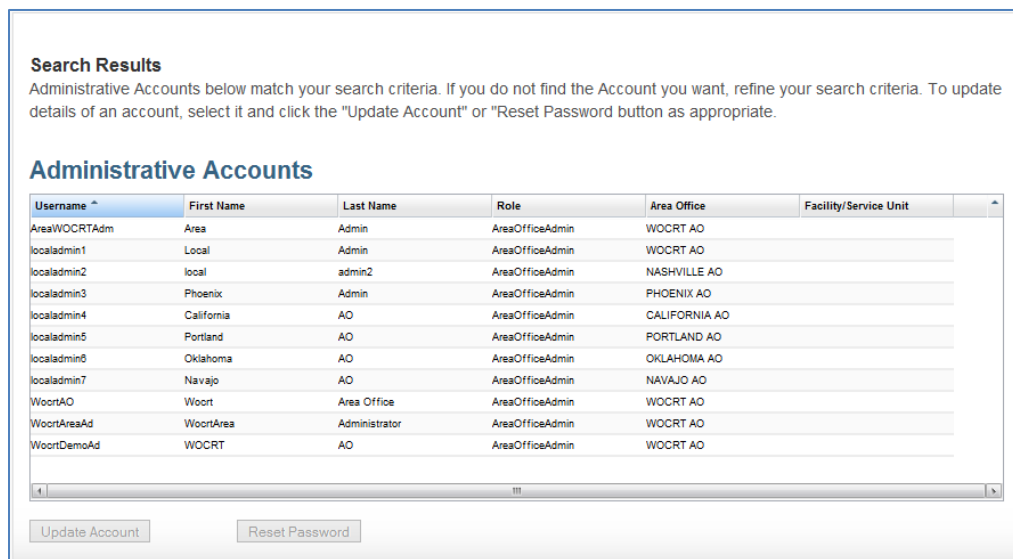   a. Click the column header again to sort the table in descending order (Figure 2-7).

Figure 2-6: Manage Administrative Account Search Results Sort Ascending Order

Figure 2-7: Manage Administrative Account Search Results Sort descending Order

2. To move a column, place the cursor in the column header, hold the left mouse button down, drag the column to the desired location, and release the left mouse button.

3. To expand or contract a column, move the cursor to the end of the column until you see the expand and compress icon (left and right arrows).

4. Hold the left mouse button down, drag the mouse left or right to the desired column width, and release the left mouse button.

5. An alternative method for sorting and configuring is to right-click on a column header and select from the menu that displays (Figure 2-8).
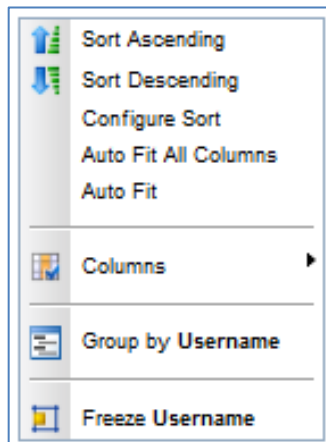
Figure 2-8: Manage Administrative Account Search Results Column Header Menu Items

   a. **Sort Ascending** and **Sort Descending** are the same as previously mentioned (step 1 and 1.a).

b. Select **Configure Sort** (Figure 2-8) to add, modify, or remove column sorting levels.
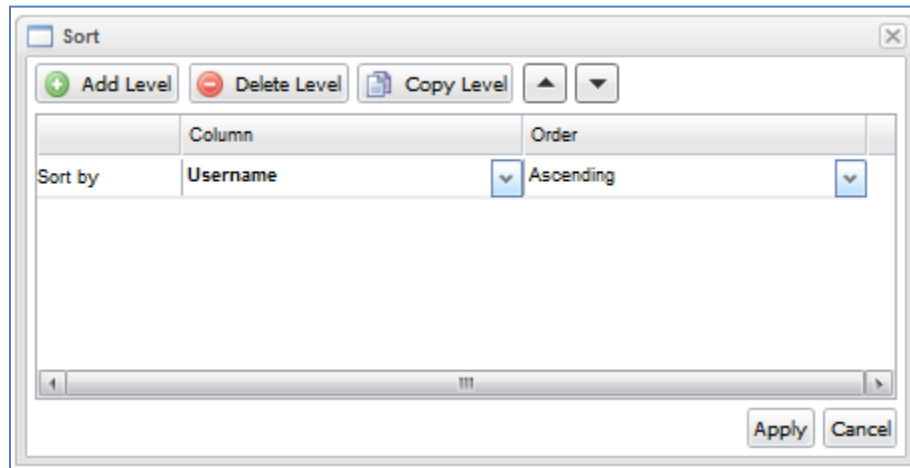
Figure 2-9: Manage Administrative Account Search Results Sort Menu Window

c. From the **Column** menu, select a column by which to sort.

d. From the **Order** menu, select the order by which to sort.

e. To add an additional sorting level, click **Add Level**.

f. To delete a sorting level, select a level from the sort list and click **Delete Level**.

g. To copy a sorting level, select a level from the sort list and click **Copy Level**.

h. To rearrange the sorting level, select a level and click the up or down arrow next to the **Copy Level** button.

i. To apply the sorting changes, click **Apply**.

j. To cancel the sorting changes, click **Cancel**.

6. Select **Auto Fit All Columns** (Figure 2-8) to set the width of each column automatically to the width of the longest row in each column.

7. Select **Auto Fit** (Figure 2-8) to set the width of the selected column to the width of the longest row

8. Select **Columns** and a **c**olumn name from the list to add (check) or remove (uncheck) from the results table (Figure 2-10 and Figure 2-11).
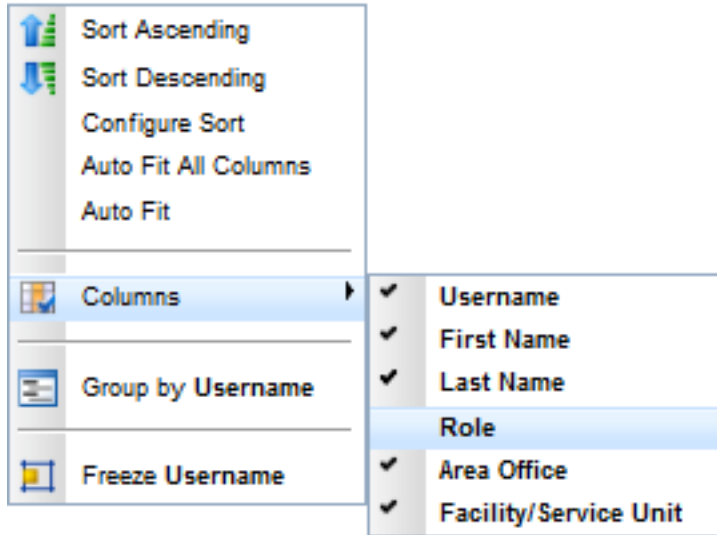
Figure 2-10: Manage Administrative Account Search Results Add or Remove Columns Menu
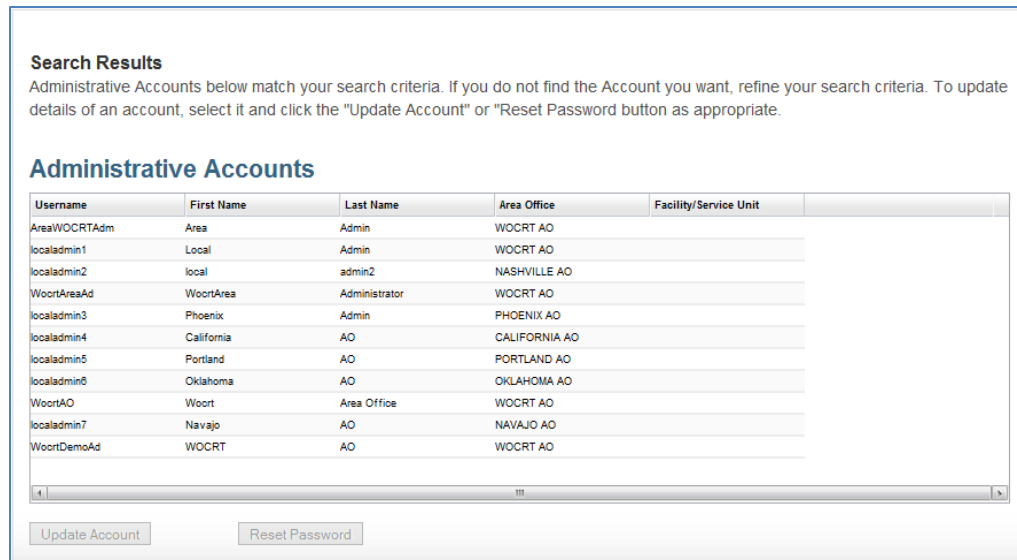
Figure 2-11: Manage Administrative Account Search Results with Role Column Removed

9. Group the results by column name by selecting **Group by** (Figure 2-8, **Group by Username**). Figure 2-12 shows the results grouped by role.
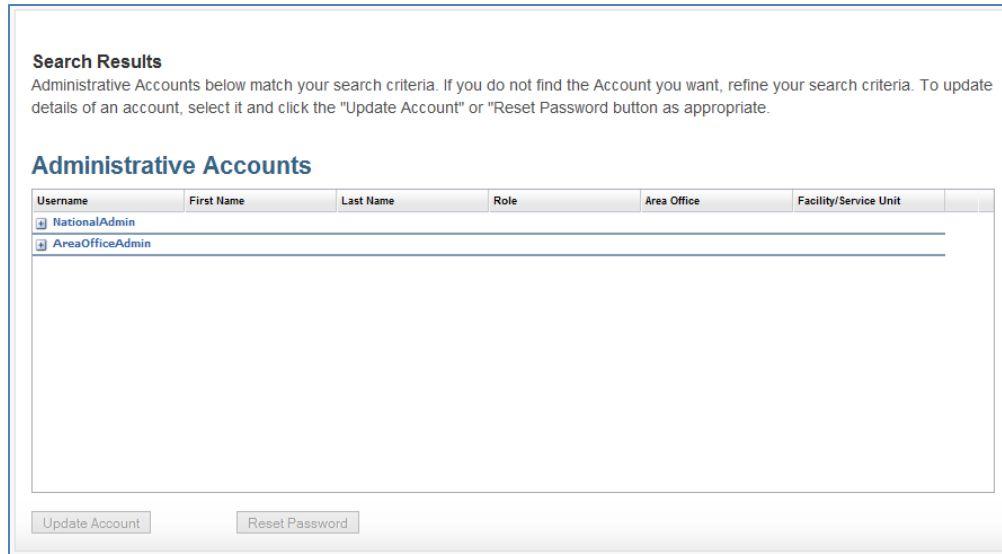
Figure 2-12: Manage Administrative Account Search Results Group Column By Role

10. Freeze the selected column by selecting **Freeze Username** (Figure 2-8). The
results table can now scroll through other columns while the **Username** column is
always visible.
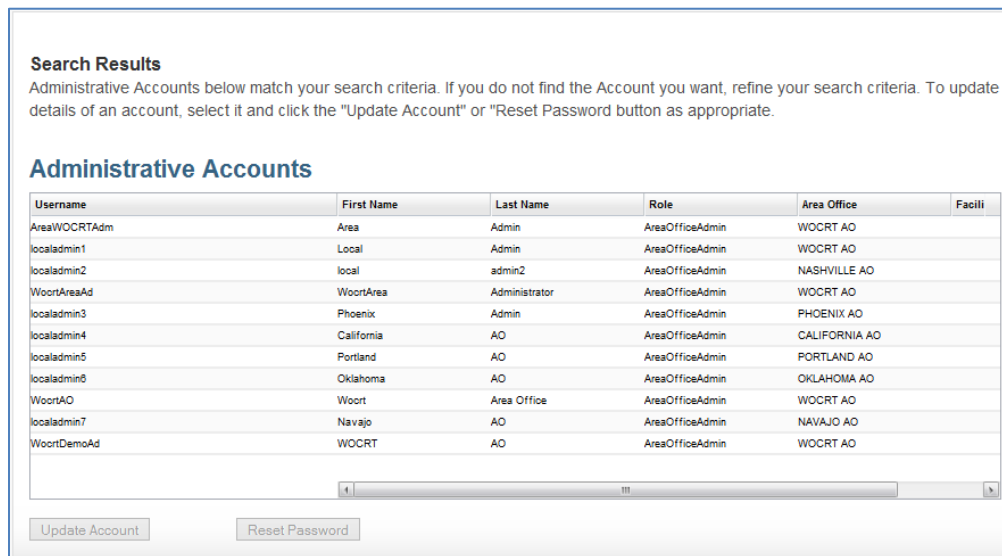
Figure 2-13: Manage Administrative Account Search Results Freeze Username Column

    a.   To unfreeze a column, right-click on the frozen column and select **Unfreeze**
from the menu (Figure 2-14).
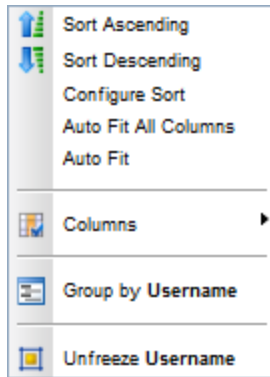
Figure 2-14: Manage Administrative Account Search Results Column Header Menu Items with the Unfreeze Option

2.5   About the PHR

To view information about the PHR, click the **About PHR** link at the bottom of the page (Figure 2-4).

2.6   Privacy Policy

To view the Website Privacy Policy, click the **Privacy Policy** link at the bottom of the page (Figure 2-4).

2.7   Terms and Conditions

To view the PHR Terms and Conditions, click the **Terms of Use** link at the bottom of the page (Figure 2-4).

2.8   Contact Us

To view information on how to contact us, click the **Contact Us** link at the bottom of the page (Figure 2-4).

2.9   Log Off

To exit the PHR Administrator Web Portal, click **Log Out** in the upper right corner of the page (Figure 2-4) or close the web browser. The Log Out link is only available after the administrator successfully logs into the PHR Administrator Web Portal.

2.10   Session Timeout

The PHR Administrator Web Portal will automatically sign the administrator out of the PHR Administrator Web Portal after 10 minutes of inactivity.

- After nine minutes of page inactivity, administrators are prompted with a PHR Session Timeout dialog (Figure 2-15) with a 60-second timer.

- To continue working in the current PHR administrative session, click **Yes, Keep me signed in**.

- To sign out of the PHR Administrator Web Portal immediately, click **No, Sign me out**.

- If neither button is clicked, the PHR Administrator Web Portal will automatically sign the administrator out of the PHR Administrator Web Portal when the **PHR Administrator Session Timeout** dialog 60-second timer reaches zero (0) seconds.

- Administrators must again logon to the PHR Administrator Web Portal to regain access to the PHR Administrator Web Portal.
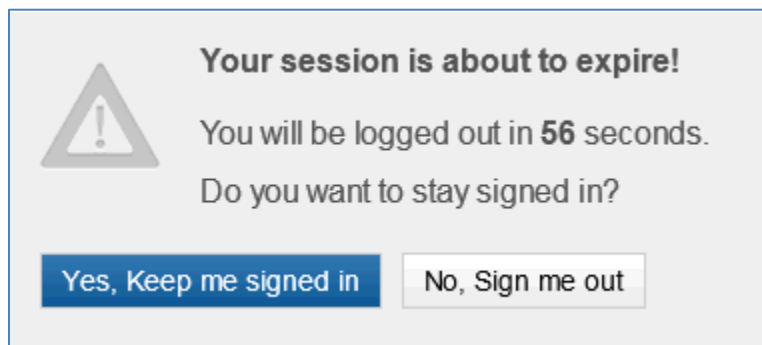
Figure 2-15: PHR Administrator Web Portal Session Timeout dialog

| **Note:** | The timeout value is reset by either selecting a different tab or clicking the **Yes, Keep me signed in** button on the PHR Session Timeout dialog message. |

3.0   Create a PHR Administrator Account

Because the PHR is not integrated with an IHS domain or the ITAC system, PHR administrators must create other administrator accounts. PHR administrators can create administrator accounts within their organizational level. Create PHR Administrative Accounts is limited to the National, AO, and SU/FA Administrator roles (see Section 1.4).

3.1   Create an AO account

1. Logon to the PHR Administrator Web Portal application as described in Section 2.0 as a National Administrator.

2. Click the **Create Account** tab. The **Create Administrative Account** page (Figure 3-1) displays.

Figure 3-1: PHR Create Administrative Account

3. Complete the form (Figure 3-1) through the **Last Name** field.

4. Select the **Role** of the administrative account as **Area Office System Administrator**.

Figure 3-2: PHR Create Administrative Account Page, Select Role

5. Select the **Area Office** for the administrator

Figure 3-3: PHR Create Administrative Account Page, Select Area Office

6. Completed **Create Administrative Account** form.

Figure 3-4: PHR Create Administrative Account Page, completed form

7. Click **Next** to create the account.

Figure 3-5: PHR Create Administrative Account Page, Select Next

3.2　Create a PHR Registrar or Service Unit System Administrator

1. Login as an **AO administrator** and follow steps 1–3 in section 3.1.

2. Select the **Area Office** for the new administrator.

3. Select either **PHR Registrar** or **Service Unit System Administrator**. The procedure is the same for both.
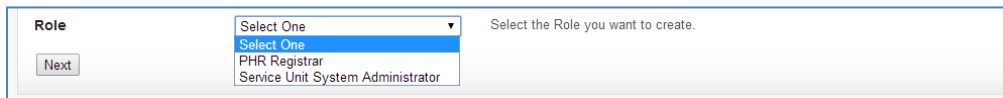
Figure 3-6: PHR Create Administrative Account Page, Select Role

4. Click on **Service Unit/Facility** and select one.
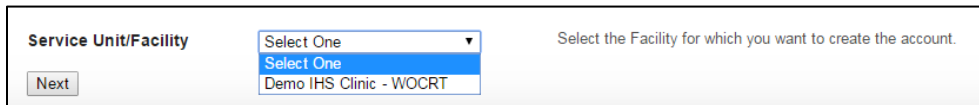
Figure 3-7: PHR Create Administrative Account Page, Select Facilities

> **Note:** PHR Administrators cannot be assigned different roles. However, the PHR Registrar and Service Unit Administrator can serve in the same role for multiple service units within the Area.

　　a. To select multiple Service Unit/Facilities, click the first **Service Unit/Facility**, hold the Control (Ctrl) key down, scroll through the list and click on each additional Service Unit/Facility.

5. Click **Next** to create the account.
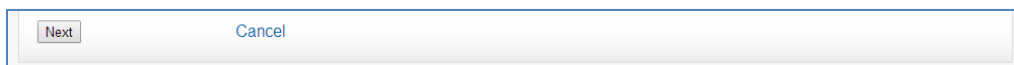
Figure 3-8: PHR Create Administrative Account Page, Click Next

3.3   Verify Account Information

The **Confirm Administrative Account** page displays after the completed form has been submitted (Figure 3-4).

1. Verify information on the **Confirm Administrative Account** page.

Figure 3-9: PHR Confirm Administrative Account

> **Note:** The confirmation will list each Service Unit/Facility the Service Unit/Facility Administrator or PHR Registrar that is selected during the account creation process for those roles.

2. If the information is correct, click **Create**.

    a. To make changes to the account information, click the **Back** button and repeat the appropriate section (3.1 or 3.2).

    b. To cancel administrative account creation, click **Cancel** and click **OK** on the Confirmation dialog to return to the **Welcome** page.
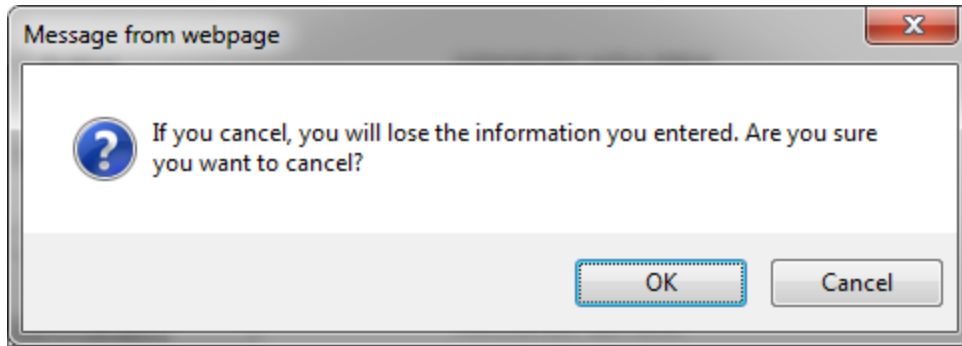
Figure 3-10: Confirmation dialog

3. Upon successful account creation, the **Administrator Account Created!** page
    displays (Figure 3-11).

    a. You may print this page by clicking **Print Details** to print the account
        information.
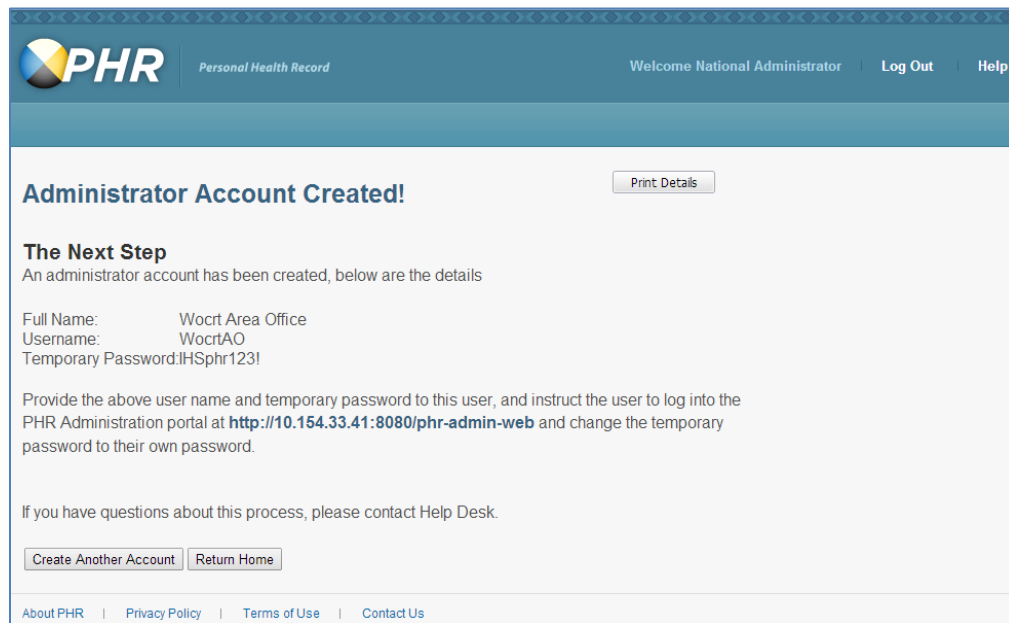
Figure 3-11: PHR Administrator Account Created

4. Contact the administrator that you created the account for and provide them with
    their account information.

> **Note:** The password is a temporary password. The administrator
> will be prompted to change their password the first time the
> administrator logs into the PHR Administrator Web Portal.

3.4   Cancel Administrative Account Creation

Cancel at any time while on the **Create Administrative Account** page by clicking **Cancel**.

Figure 3-12: PHR Create Administrative Account Page, Cancel

Click **OK** on the Confirmation dialog to return to the **Welcome** page.
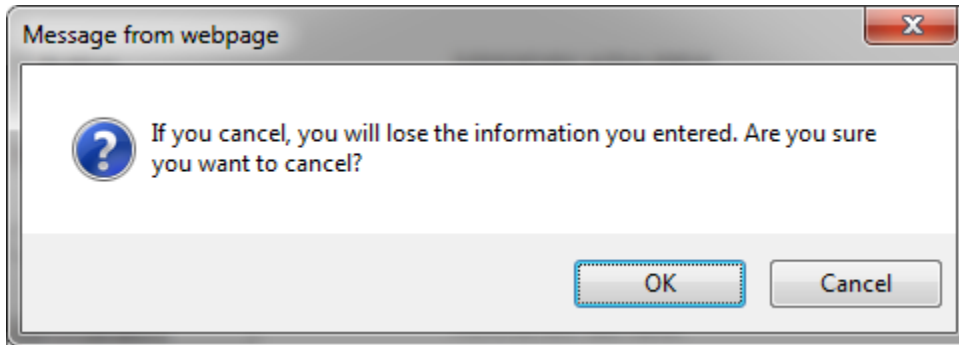
Figure 3-13: Confirmation dialog

4.0   Manage PHR Administrative Accounts

Because the PHR is not integrated with an IHS domain or the ITAC system, PHR administrators may need to update other administrator accounts. This functionality is limited to the National, AO, and SU/FA Administrator roles (see Section 1.4 for role details). Manage accounts allow these administrative roles to update other PHR administrators' active status, name, role, Area office, and service unit/facility and reset other PHR administrators' password.

Updating PHR Administrative accounts is role specific and limited to the following:

- **National Administrators**: These administrators can update other National Administrators and AO Administrators.

- **AO Administrators**: These administrators can update Service Unit/Facility Administrators and PHR Registrars within their area. For example, a California PHR AO Admin cannot update SU/FA or PHR Registrar accounts for Service Units/Facilities that are included in the Phoenix Area.

- **Service Unit/Facility Administrators**: These administrators can update PHR Registrars within their assigned Service Units/Facilities. For example, if a SU/FA is assigned to one SU/F, then they can only update PHR Registrar accounts for that SU/F.

- **PHR Registrars**: These administrators cannot update any PHR Administrator accounts.

4.1   Search for Administrative Account

1. Logon to the PHR Administrator Web Portal application as defined in Section 2.0.

> **Note:** Logon to the portal based on the administrator account being managed. For example, if the administrative account being managed is an AO Administrator, logon to the portal as a National Administrator.

2. Click the **Manage Account** tab. The **Manage Administrative Account** page (Figure 4-1) displays.

Figure 4-1: PHR Manage Account

3. Search for the administrator account to manage in the **Search For Administrative Account** pane by entering one or more of the following on the **Manage Administrative Account** page:

    - Username

    - Last Name

    - First Name

    - Middle Name

    > **Note:** The asterisk (*) symbol can be used as a wildcard to replace zero or more characters in a word. For example, to search for accounts with a last name that begins with "Demo" type "Demo*" in the last name field. The search results will display every administrator user with the selected role that begins with Demo, such as Demo, Demos, Demotest, Demouser, demoprovider, and etc.

4. (Optional) Select one or more roles in the **Role** field. The roles available will depend on the type of administrative logon.

    - National Administrators can select the **Area Office Admin** or **National Admin** role (Figure 4-2).

Figure 4-2: Manage Administrative Account - National Administrators Search Role Field: Area Office Admin and National Admin

- AO Administrators can select the **Registrar** or **Service Unit Admin** role (Figure 4-3).

Figure 4-3: Manage Administrative Account - AO Administrators Search Role Field: Registrar and Service Unit Admin

- SU/FA Administrators can select the **Registrar** role (Figure 4-4).

Figure 4-4: Manage Administrative Account – SU/FA Administrators Search Role Field: Registrar

5. Do one of the following: click **Search** or **Clear** (Figure 4-5). After clicking **Search**, the **Manage Administrative Account** - Search Results Pane will open (Figure 4-6).

Figure 4-5: Manage Administrative Account - Search and Clear Buttons
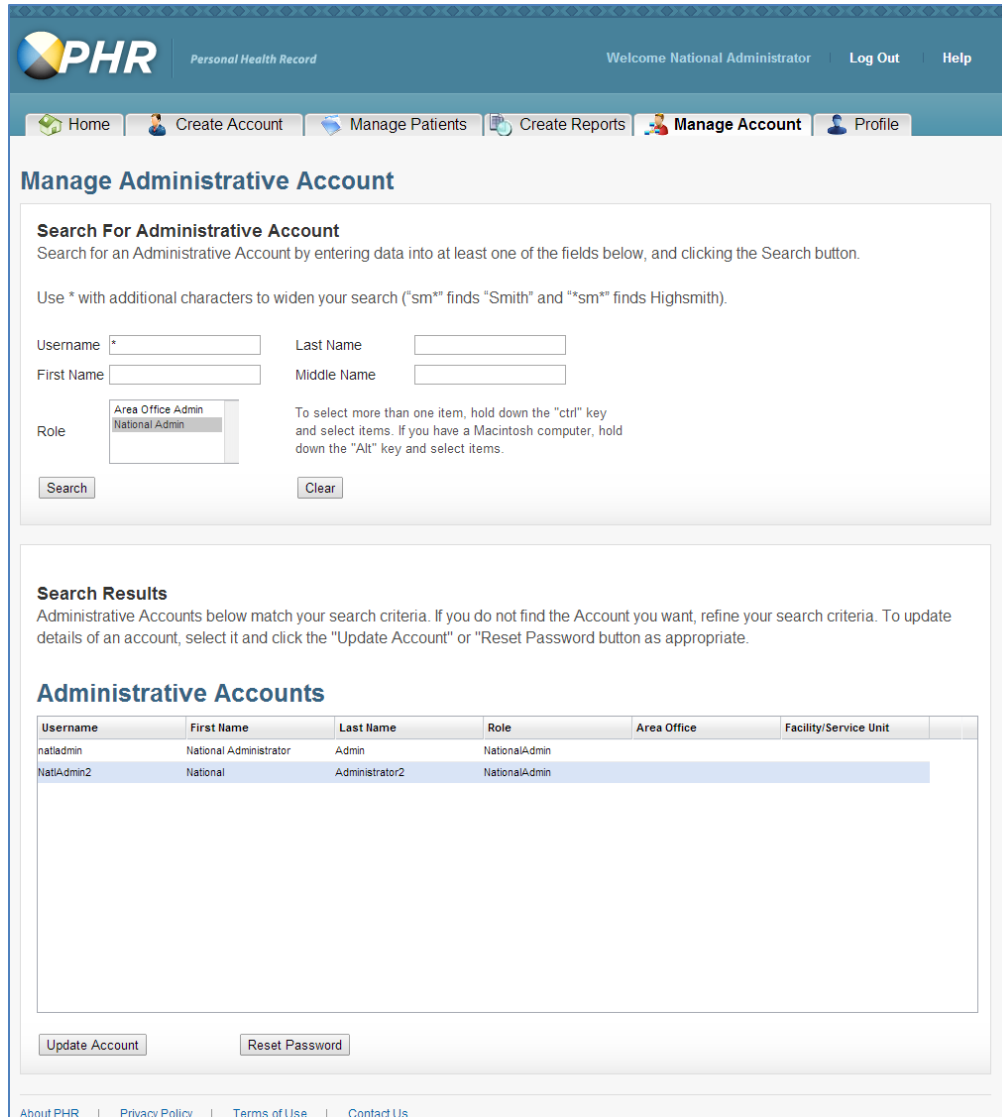
Figure 4-6: Manage Administrative Account - Search Results Pane

6. (Optional) Sort or modify the search results in the **Search Results** pane (Section 2.4).

7. Select an account to manage from the **Search Results** pane below the **Search For Administrative Account** pane and do one of the following:

- Click **Update Account** to update the selected administrative account and complete the steps in Section 7.0.

- Click **Reset Password** to reset the password of the selected administrative account and complete the steps in Section 4.4.

4.2   Update Administrator Account

Because the PHR is not integrated with an IHS domain or the ITAC system, PHR administrators may need to update other administrator accounts. This functionality is limited to the National, AO, and SU/FA Administrator roles (see Section 1.4 for role details). The **Update Administrative Account** page allows these administrators to update other PHR administrators' active status, name, role, area office, and service unit/facility.

1. Complete the steps in Section 4.1. The **Update Administrative Account** page displays (Figure 4-7).

Figure 4-7: Update Administrative Account

2. Do one or more of the following on the **Update Administrative Account** page:

   a. Disable the selected administrator account by unchecking the **Active** check box.

   b. Enable the selected administrator account by checking the **Active** check box.

   c. Update the administrator's name by updating the text in the **First Name**, **Middle Name**, or **Last Name** text fields.

   d. To update the administrator's role, select a role from the **Role** menu.

e. To update the administrator's SU/F, select a **Service Unit/Facility** from the menu.

3. To continue with the update, click **Next**.

   a. To cancel the update, click **Cancel** and click **OK** on the **Confirmation** dialog to return to the **Manage Administrative Account** page.

4.3 Confirm Changes

1. After clicking **Next** (Section 4.2, step 3), the **Confirm Update Administrative Account** page displays.

Figure 4-8:Confirm Update Administrative Account

2. Click **Confirm** if the information is correct (Figure 4-8).

3. To make changes to the updated administrative account information, click the **Back** button (Figure 4-8) and repeat Section 4.2.

   a. To cancel the update, click **Cancel** (Figure 4-8) and click **OK** on the **Confirmation** dialog (Figure 4-9) to return to the Manage Administrative Account page.

   b. To go back to the **Confirm Update Administrative Account** page and continue updating the administrative account, click **Cancel** on the **Confirmation** dialog (Figure 4-9).
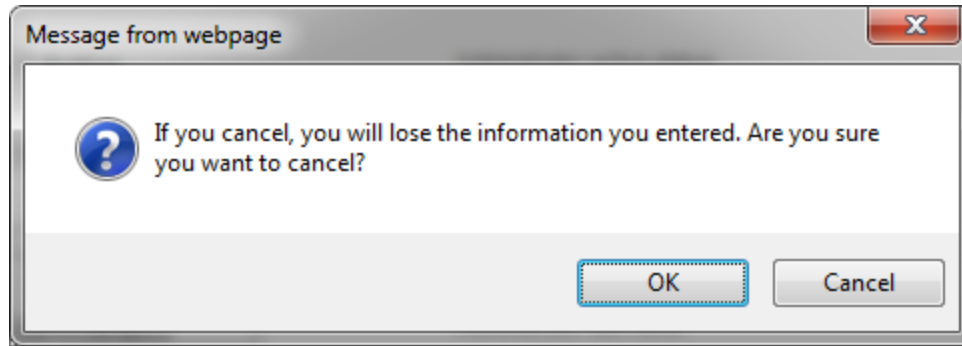
Figure 4-9: Confirmation dialog

4. When you are finished updating, do one of the following:

   a. Click **Log Out** in the upper right corner to log off of the PHR Administrator Web Portal application (Figure 4-8).

   b. Click **Help** in the upper right corner (Figure 4-8) to access the PHR Administrator Web Portal application help function.

   c. Click **Print** (Figure 4-8) to print the updated account information. The **Question** dialog will display.

      • To continue the print option, click **Yes** on the **Question** dialog (Figure 4-10) to display the **Print Preview** window (Figure 4-11).

Figure 4-10: Print – Question dialog

      • To go back to the Confirm Administrative Account Updated, click **No** or click the in the upper right corner on the Question dialog.

   d. Click **Print** to print the details of the account created.

      • To cancel the print, click the in the upper right corner of the **Print Preview** window.

Figure 4-11: Print - Print Preview Window

4.4   Reset Administrative Account Password

Because the PHR is not integrated with an IHS domain or the ITAC system, PHR administrators may need to reset the password for other administrator accounts. This functionality is limited to the National, AO, and SU/FA Administrator roles (see Section 1.4 for role details). The **Reset Password for Administrative Account** page allows these administrators to reset the password of other PHR administrators.

> **Note:** Administrators resetting password requests for another PHR Administrator must verify the identity of the Administrator requesting the password reset. In-person verification is preferred. If in-person verification is not possible, a series of questions can be asked to establish identity, or ask the supervisor to submit a password reset request, or follow HIPAA and/or facility procedures for establishing identity. The PHR Administrator requesting the password reset shall certify in writing that they are the individual who they claim to be, and they understand that the knowing and willful request for or acquisition of a record under false pretenses is a criminal offense under the Privacy Act and subject to a fine of not more than $5,000. (5 U.S.C. 552a).

1. Complete Steps 1–7 of Section 4.1.

2. Reset the password of the selected administrator account on the **Reset Password for Administrative Account** page (Figure 4-12) by entering a new password in the **New Password** field and enter the same password in the **Confirm New Password** field.

> **Note:** The new password must meet the requirements as defined on the **Reset Password for Administrative Account** page.
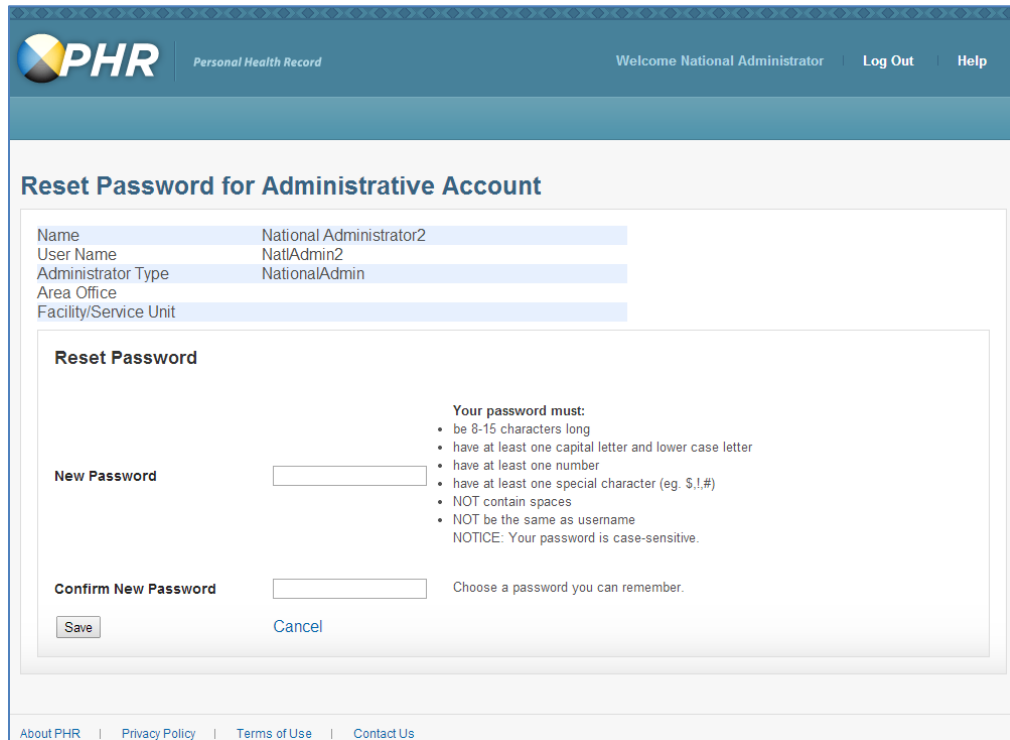
Figure 4-12: Manage Administrative Account - Reset Password for Administrative Account

3. Click **Save**. If the reset is successful, the **Confirm Administrative Account Updated** page (Figure 4-14) displays.

   a. If the new password entered has been used in one of the previous six password resets or updates, the password will not be accepted and the **You cannot reuse the last 6 passwords** dialog will open (Figure 4-13). Click **OK** on the Passwords dialog and repeat Steps 2 and 3.
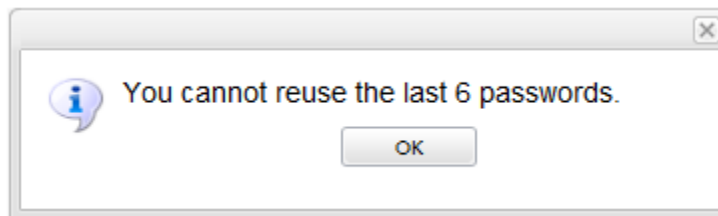
Figure 4-13: You cannot reuse the last 6 passwords dialog

   b. To cancel the password reset, click **Cancel** (Figure 4-12) and click **OK** on the **Confirmation** dialog to return to the **Manage Administrative Account** page.
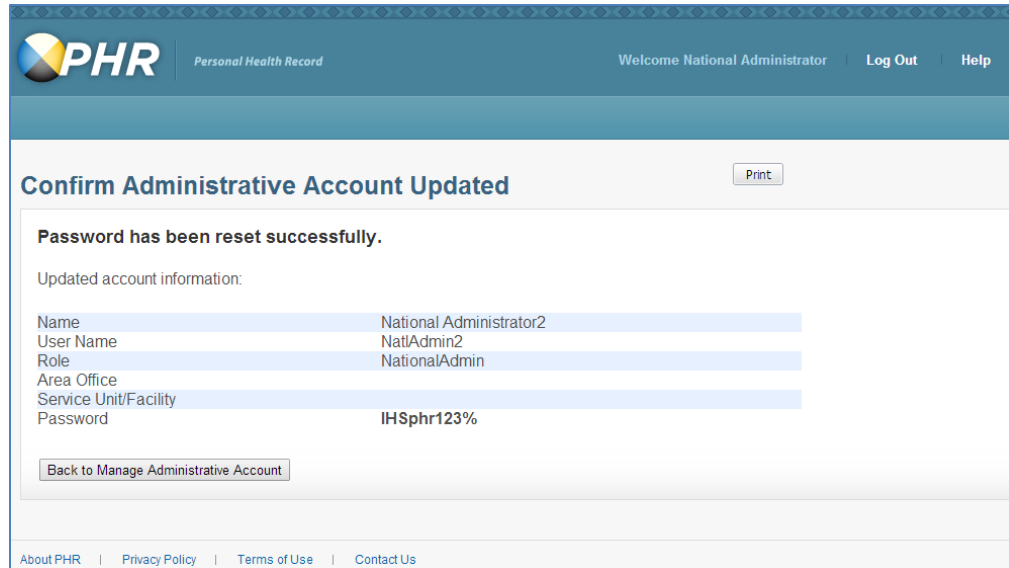
Figure 4-14: Manage Administrative Account - Confirm Administrative Account Updated

4. Contact the administrator who you are resetting the password for that their
   account has been updated and provide them with the new password.

> **Note:** The new password is a temporary password. The
> administrator will be asked to change their password the
> next time the administrator logs into the PHR
> Administrator Web Portal.

5. When you are finished updating, do one of the following on the **Confirm
   Administrative Account Updated** page (Figure 4-14):

   a. Click **Back to Manage Administrative Account**.

   b. Click **Log Out** in the upper right corner to log off of the PHR Administrator
      Web Portal application.

   c. Click **Help** in the upper right corner to access the PHR Administrator Web
      Portal application help function.

   d. Click **Print** to print the updated account information. The Question dialog
      opens (Figure 4-15).

      • To continue the print option, click **Yes** on the **Question** dialog to display
        the **Print Preview** window (Figure 4-16).

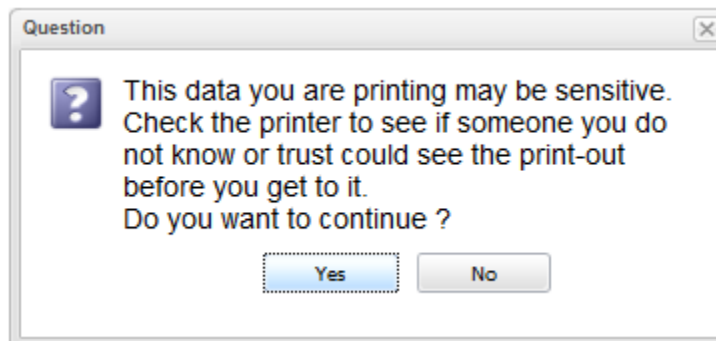   • To go back to the **Confirm Administrative Account Updated**, click **No**
        or click the in the upper right corner on the **Question** dialog.
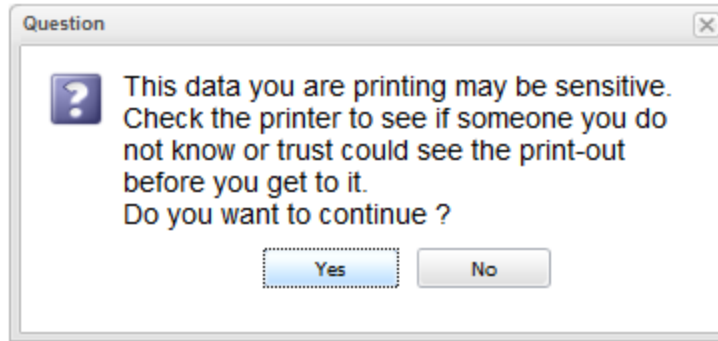
Figure 4-15: Print - Question dialog

- To print the details of the account created, click **Print** on the **Print Preview** window (Figure 4-16).

- To cancel the print, click the in the upper right corner of the **Print Preview** window.
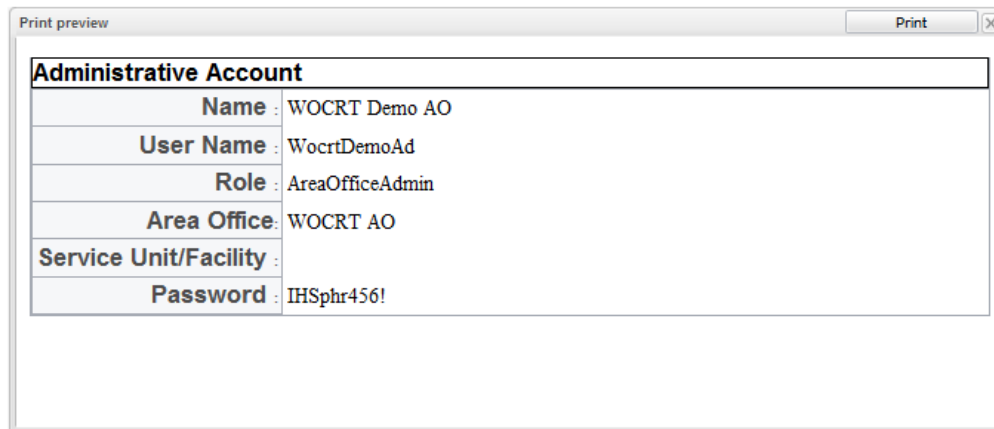
Figure 4-16: Print - Print Preview Window

6. Contact the administrator who you are resetting the password for that their account has been updated and provide them with the new password.

> **Note:** The new password is a temporary password. The administrator will be asked to change their password the next time the administrator logs into the PHR Administrator Web Portal.

4.5   Unlock Administrative Account

Because the PHR is not integrated with an IHS domain or the ITAC system, PHR administrators may need to reset the password for other administrator accounts to unlock the account. This functionality is limited to the National, AO, and SU/FA Administrator roles (see Section 1.4 for role details). To unlock an administrative account, complete the steps in Section 4.4.

Web Portal Administrator Manual   Manage PHR Administrative Accounts
September 2020

35

> **Note:** Administrators unlocking locked administrative accounts for another PHR Administrator must verify the identity of the Administrator requesting the password reset. In-person verification is preferred. If in-person verification is not possible, a series of questions can be asked to establish identity, or ask the supervisor to submit a PHR unlock Administrative account reset request, or follow HIPAA and/or facility procedures for establishing identity. The PHR Administrator requesting the account unlock shall certify in writing that they are the individual who they claim to be, and they understand that the knowing and willful request for or acquisition of a record under false pretenses is a criminal offense under the Privacy Act and subject to a fine of not more than $5,000. (5 U.S.C. 552a).

5.0   Change Account Password

Because the PHR is not integrated with an IHS domain or the ITAC system, PHR administrators may need to update their own password. PHR Administrator accounts expire every 60 days and will be prompted to change their password at least 10 days in advance. If the administrator's password expires or the administrator has their password reset by an up-level PHR Administrator, the administrator will be prompted to reset their password at the next logon.

> **Note:** Passwords for new PHR Administrators and administrators who had their password reset by an up-level PHR Administrator are temporary and expire within 10 days. If these passwords expire, the administrator will need to have the password reset by an up-level PHR Administrator.

5.1   Non-Expired Password Reset

To change your administrator account password:

1. Logon to the PHR Administrator Web Portal application as described in Section 2.0.
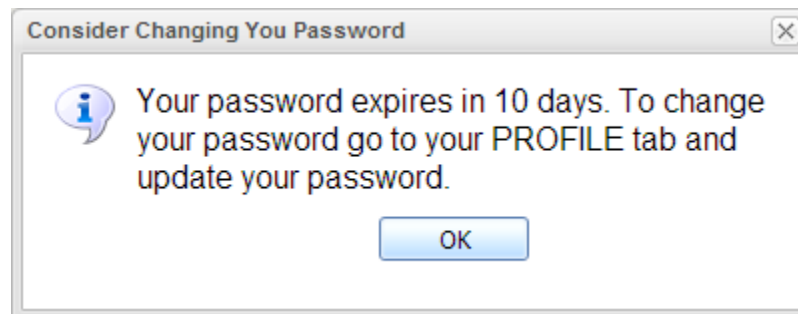
Figure 5-1: Consider Changing Your Password dialog

2. If the **Consider Changing You Password** dialog opens, click **OK**. The **Welcome to your Personal Health Record (PHR)!** page (Figure 5-2) opens.

Figure 5-2: PHR Welcome

3.   Click the **Profile** tab. The **Profile** page (Figure 5-3) displays.
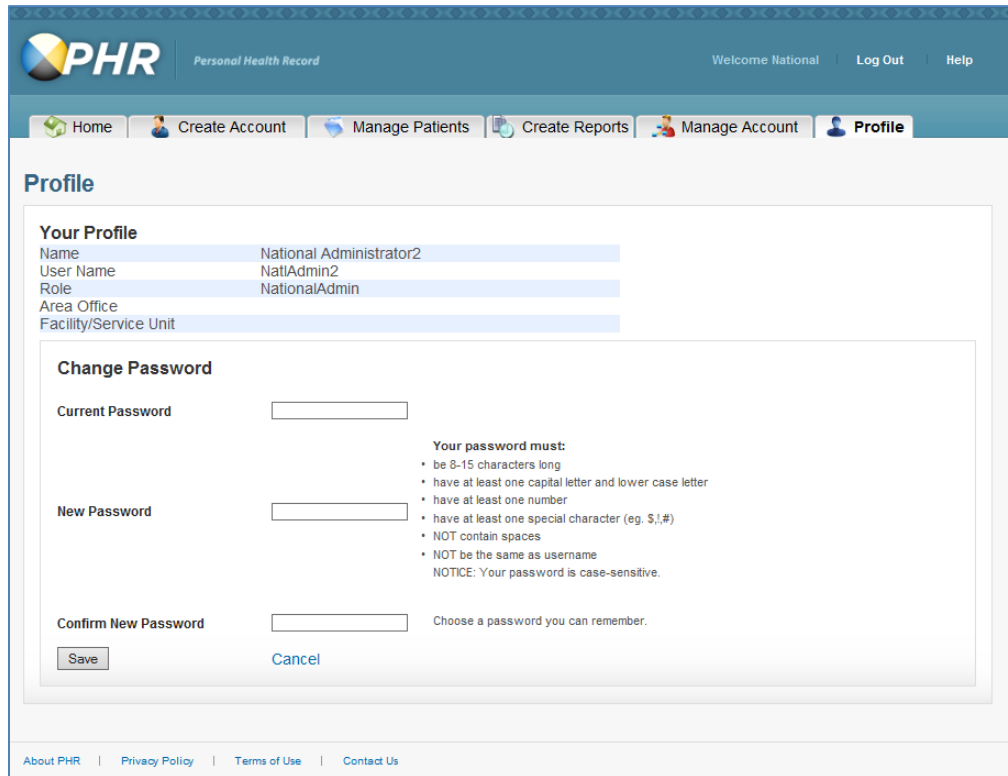
Figure 5-3: Profile – Change Password

4.   Type your current password in the **Current Password** field.

5.   Type new password in the **New Password** field.

6.   Retype the new password in the **Confirm New Password** field.

7. Click **Save** to save your password. The **Changed Password Confirmation** dialog opens (Figure 5-4).
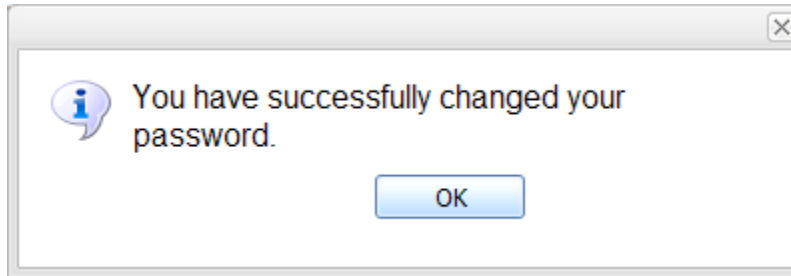
Figure 5-4: Changed Password Confirmation Dialog

8. Click **OK** on the **Password** dialog (Figure 5-4) to return to the **Profile** page.

   a. To cancel the password reset and return to the **Welcome** page, click **Cancel** on the **Profile** page (Figure 5-3) and click **OK** on the Password confirmation dialog.

5.2   Forced Password Reset

If the administrator's password expires or the administrator has their password reset to a temporary password by an up-level PHR Administrator, the administrator will be prompted to reset their password at the next logon.

To change your administrator account password:

1. Logon to the PHR Administrator Web Portal application as defined in Section 2.0. The **Change Password** page (Figure 5-5) displays.

Figure 5-5: Change Password

2. Type the new password in the **New Password** field.

3. Retype the new password in the **Confirm New Password** field.

4. Click **Save** to save your password. The Confirmation Dialog (Figure 5-6) opens.
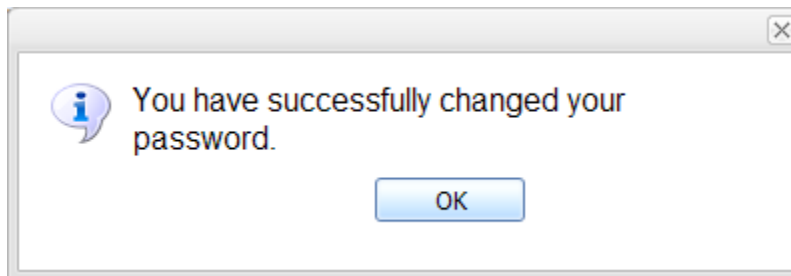
Figure 5-6: Changed Password Confirmation dialog

5. Click **OK**. The **Welcome to you Person Health Record (PHR)!** page (Figure 5-2) is displayed.

   a. To cancel the password reset and return to the **PHR Administrator Login** page, click **Cancel** (Figure 5-2) and click **OK** on the confirmation dialog (Figure 5-7).

   b. To go back to the **Change Password** page and continue resetting the account password, click **Cancel** on the confirmation dialog (Figure 5-7).
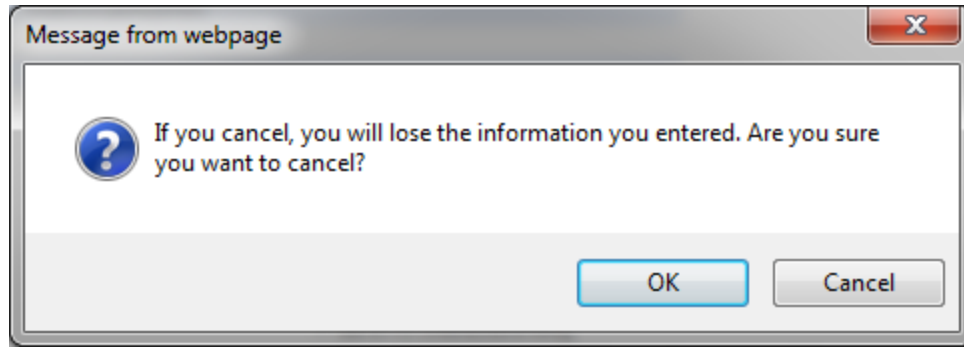
Figure 5-7: Confirmation dialog

6.0   Process PHR Patient Applications

The PHR Registrar is the only role that can process a patient's PHR Application.

Before patients can access the PHR and view their IHS Medical Record, the patient will need to complete the following steps:

1. Register to use the PHR online at https://phr.ihs.gov.

2. The patient goes to their IHS facility to complete the in-person identity verification process.

   a. The PHR Registrar verifies the patient's identity

3. The PHR Registrar processes the patient's application and links the patient's registered PHR account with their IHS Medical Record.

4. The patient logs on to the PHR at https://phr.ihs.gov.

See Section 1.4 for the PHR Registrar role definitions. Once the patient's PHR application has been processed, the patient can logon to the PHR and view their IHS Medical Record information for the selected facility. This information includes an appointment list, demographic information, medication list, health issues, test results, immunizations, vital signs, send and receive secure messages, procedures, goals, medical devices, hospital admissions, and download health information.

6.1   Process Application: Step 1: Register to Use PHR

Patients must complete the PHR online registration process before the PHR Registrar can process the patient's PHR application.

To register patients to use the PHR, follow these steps:

1. Go to the patient PHR Patient Web Portal application website at https://phr.ihs.gov.

Figure 6-1: PHR Patient Web Portal application logon

2. Click **Register to use PHR**. The **Step 1: Create Your Account** page displays (Figure 6-2).
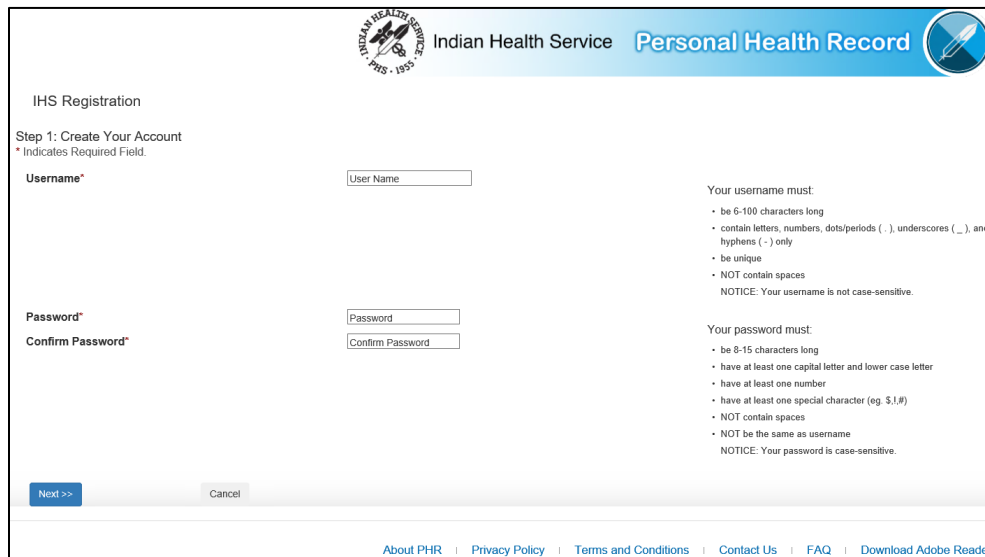
Figure 6-2: PHR Patient Web Portal application Step 1: Create Your Account

3. Complete the form on the **Step 1: Create Your Account** page by following the instructions on the page.

4. Click **Next** to continue. The **Step 2: Your Security Questions and Answers** page displays (Figure 6-3).

    a. Click **Cancel** to return to the PHR Patient Web Portal application logon page. You may do this at any of the steps in the process.

5. Complete the form on the **Step 2: Your Security Questions and Answers** page by selecting three security questions from the dropdown and typing an answer for each question in the security answer boxes.

Figure 6-3: PHR Patient Web Portal application Step 2: Your security questions and answers

6. Click **Next** to continue. The Step 3: **Enter Your Information** page displays (Figure 6-4).

    a. To go back to the **Step 1: Create Your Account** page, click **Previous**. You may go to the previous page at any of the steps in the process.

Figure 6-4: PHR Patient Web Portal application Step 3: Enter your information

7. Complete the form on the **Step 3: Enter Your Information** page by following the instructions on the page.

> **Note:** Fields marked with a red asterisk (*****) are required fields. Additional information provided will help the PHR Registrar minimize the time to process the PHR application.

8. Click **Next** to continue. The **IHS.gov Privacy Policy Statement** page displays (Figure 6-5).
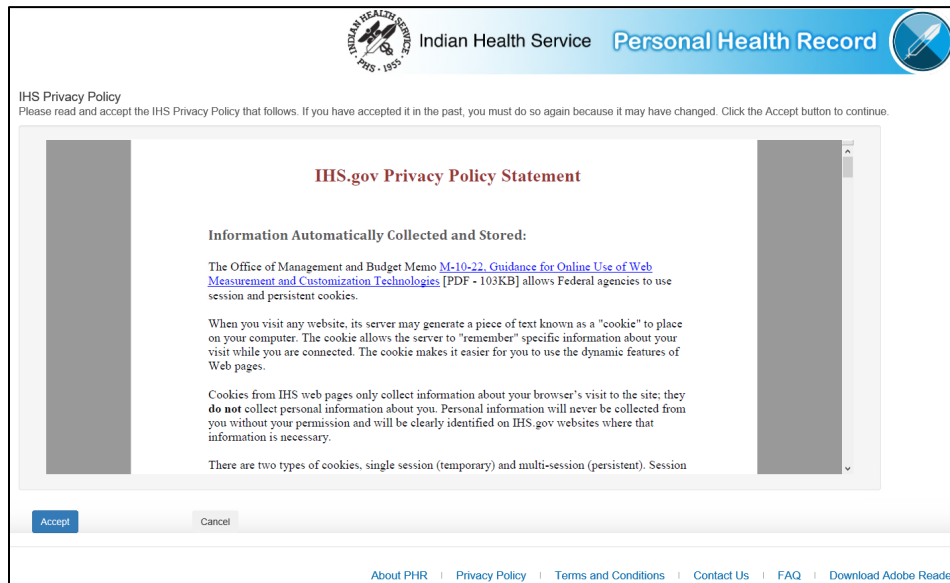
Figure 6-5: PHR Patient Web Portal application IHS Privacy Policy Statement

9. Registering PHR users must accept the IHS.gov Privacy Policy Statement as part of the registration process. Read the statement and click **Accept** to continue. The **IHS Terms and Conditions** page displays (Figure 6-6).

   a. Click **Cancel** to return to the PHR Patient Web Portal application logon page.
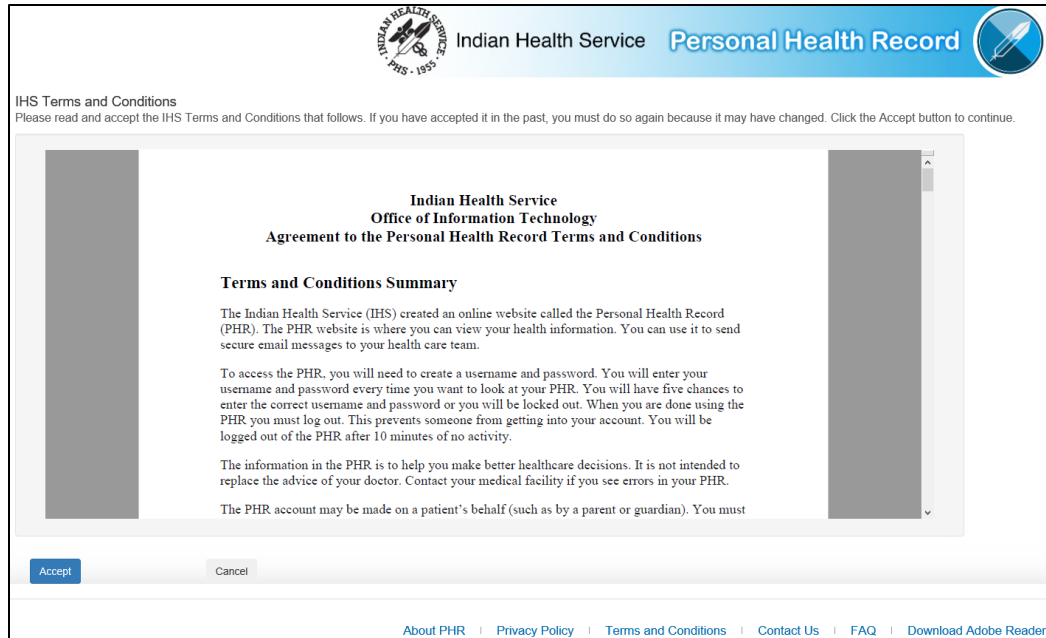
Figure 6-6: PHR Patient Web Portal application IHS Terms and Conditions

10. Registering PHR users must accept the IHS Terms and Conditions as part of the registration process. Read the statement and click **Accept** to continue. The **Final Step: Confirm Your Information** page displays (Figure 6-7).
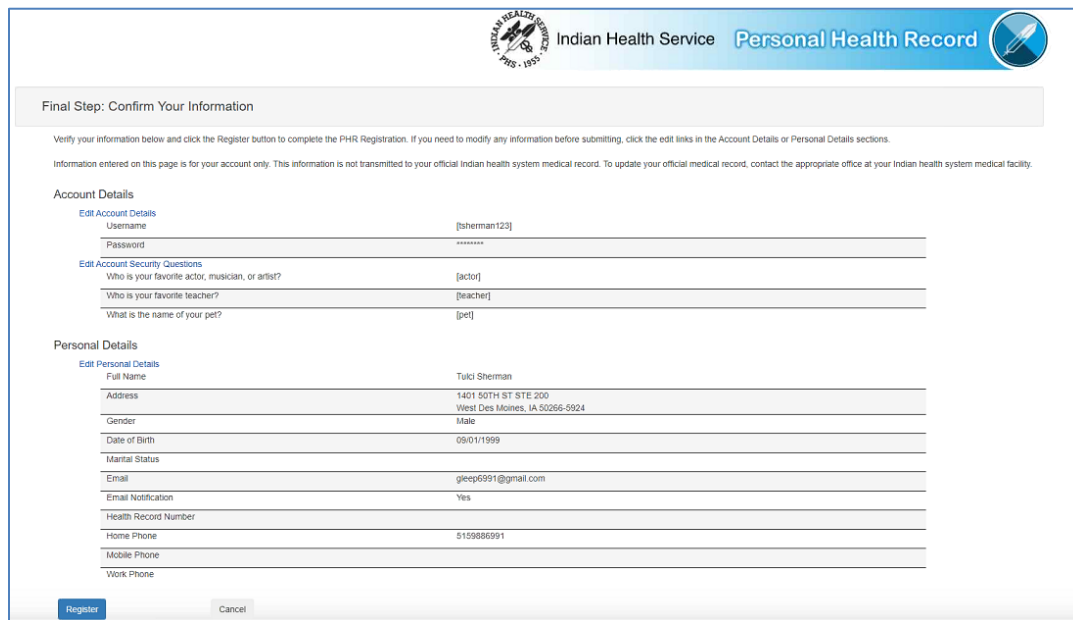
Figure 6-7: PHR Patient Web Portal application Final Step: Confirm Your Information

11. Confirm the information entered during the PHR patient registration process on the **Final Step: Confirm Your Information page** by doing one of the following or click **Cancel** to return to the PHR Patient Web Portal application logon page.

a. Click **Register** to complete the registration. The **Next Steps** page displays (Figure 6-8).

b. Click **Edit Account Details** and repeat Steps 3 through 10.

c. Click **Edit Account Security Questions** and repeat Steps 5 through 10.

d. Click **Edit Personal Details** and repeat Steps 7 through 10.

> **Note:** The patient must click **Register** to create an account for PHR access.
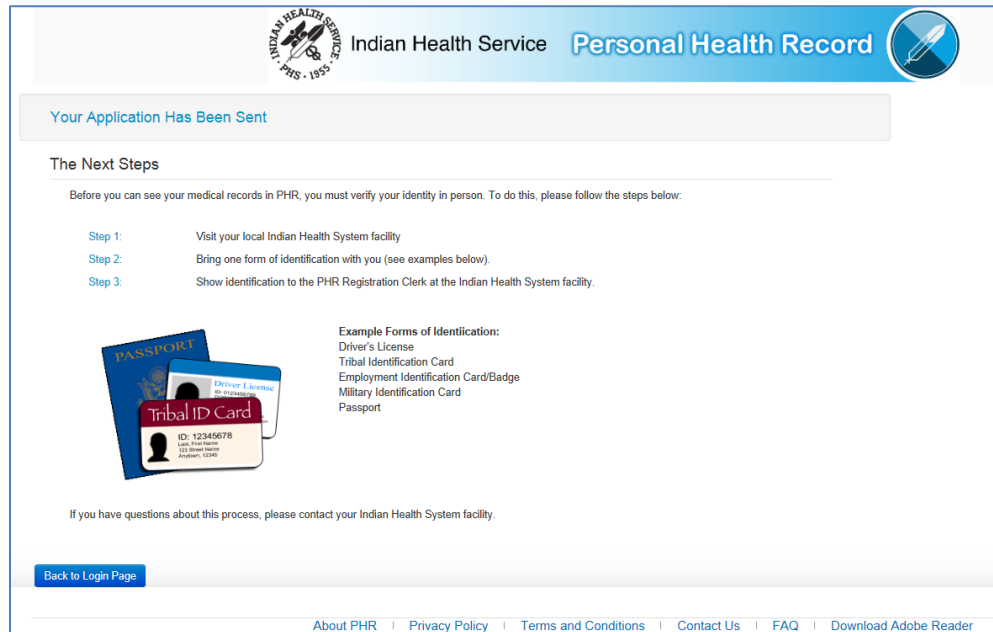
Figure 6-8: PHR Patient Web Portal application Next Steps

12. Follow the instructions on the **Next Steps** page to complete the registration process.

13. Close the window or click **Back to Logon Page** to return to the PHR Patient Web Portal application logon page.

> **Note:** At this point, the patient's PHR account is created and the patient can log into the PHR. Until the patient's identity is verified and the application is processed, the patient will see this page (Figure 6-8) and cannot view the IHS Medical Record.

6.2   Process Application: Step 2: Verify Identity

Once the patient completes the PHR online registration process, the patient is informed that their identity needs to be verified in person before they can view their IHS Medical Record through the PHR.

The PHR Registrar is responsible for verifying the patient's identity in-person. The PHR Registrar must follow the facility's existing policies and procedures that pertain to the [Procedure for Verification of Identity Prior to Disclosure of PHI](https://www.ihs.gov/ihm/pc/part-2/chapter-7-health-insurance-portability-and-accountability-act-privacy-rule-and-the-privacy-act/#2-7.24) (https://www.ihs.gov/ihm/pc/part-2/chapter-7-health-insurance-portability-and-accountability-act-privacy-rule-and-the-privacy-act/#2-7.24) to verify the identity of the patients requesting access to their PHR.

Forms of identification include the following:

- If the identity of the patient requesting PHR access is personally known to the responsible the PHR Registrar, the patient's representation regarding their identity will be sufficient verification if it is reasonable under the circumstances. Otherwise, upon completing the Form IHS-810, the patient's identity shall be verified as follows:

- Provide one piece of tangible identification (preferably picture I.D.)

  – Driver's license
  – military identification card
  – tribal identification card
  – employment identification card/badge
  – passport
  – alien registration card

- If a patient is requesting his or her own PHR, the name on the identification must match the name of the patient whose record is being sought.

- If the patient's name has been legally changed, evidence documenting the name change must be presented. Additionally, the patient shall provide particulars that can be verified by information already included in the record, such as place of birth, names of parents, an occupation, rank attained in Uniformed Services, or specific times the patient received medical treatment.

- If the patient cannot produce identification, in addition to providing the particulars noted above, they shall certify in writing that they are the individual who they claim to be, and they understand that the knowing and willful request for or acquisition of a record under false pretenses is a criminal offense under the Privacy Act and subject to a fine of not more than $5,000. (5 U.S.C. 552a (I)).

- An individual who makes a request for PHR access on behalf of a minor, a person who is legally incompetent, or another individual, shall verify that he/she has authority to act by providing a copy of a birth certificate, a court order, or other competent evidence of the relationship or authority, e.g., health care power of attorney, in addition to verifying their own identity with photo identification (unless personally known to the PHR Registrar), unless the PHR Registrar can establish that evidence of the relationship or authority has previously been provided. The type of identification and any documentation of authority used will be documented on the completed Form IHS-810, e.g., "verified, Driver's License." The PHR Registrar making the verification must initial and date the form. See Section 10.0 for more details on requesting and granting PHR access for minors.

> **Note:** If the patient is unable to verify their identity, you must stop processing the patient's PHR application until the patient can prove their identity.

Once the patient's identity has been verified, the PHR Registrar can process the patient's PHR application (see Section 6.3).

6.3   Process Application: Step 3: Link Accounts

Process Application is limited to the PHR **Registrar**. Processing the patient's PHR will allow patients to view their IHS Medical Record. Patients must verify their identity before the PHR Registrar can process their PHR application (see Section 9.0).

> **Note:** The patient does not have to be a patient at your SU/FA to process a patient's PHR Application; however, the patient's IHS SU/FA must have on-boarded with the IHS MPI and IHS HIE.

6.3.1   Find Patient Account

1. Logon to the PHR Administrator Web Portal application as the PHR **Registrar** as defined in Section 2.0. The Welcome page - PHR Registrar view opens (Figure 6-9).

Figure 6-9: Welcome page - PHR Registrar view

2. Click the **Process Application** tab. The Process Application page- Search for
   Patient Records pane (Figure 6-10).
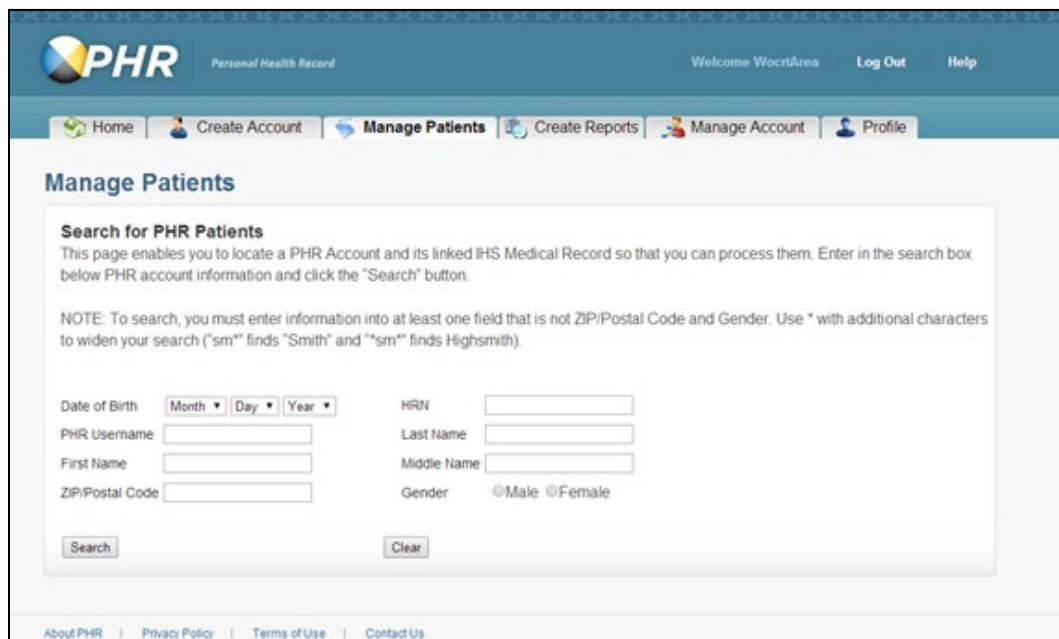
Figure 6-10: Process Application - Search for Patient Records pane

3. Search for the patient's account to process the application in the **Search for
   Patient Records** pane by entering one or more of the following on the Process
   Application page:

   - First Name

   - Date of Birth

   - Middle Name

- ZIP/Postal Code

- Gender

> **Note:** The asterisk (*****) symbol can be used as a wildcard to replace zero or more characters in a word. For example, to search for accounts with a last name that begins with "Demo" type "Demo*" in the last name field. The search results will display every PHR registered account that begins with Demo, such as Demo, Demos, Demotest, Demouser, demoprovider, and etc. The more demographic data entered in the Search for Patient Records pane, the results will match the patient's demographic information better.

4. Click **Search** (Figure 6-10) to return the matching results or click **Clear** to clear the search fields. The Manage Patient – Search Results pane opens (Figure 6-11).

Search Results
Below are the results of your search. Highlight the "right" PHR Account and click "View Selected Record" to view it and its linked IHS Medical Record. If you do not see the "right" PHR Account, then refine your search.

	Name	Date of Birth	User Name	HRN	Gender	Address
🔗	Jones, Isabella	05/01/1947	IsaJones		Female	1357 Amber Drive

View Selected Record
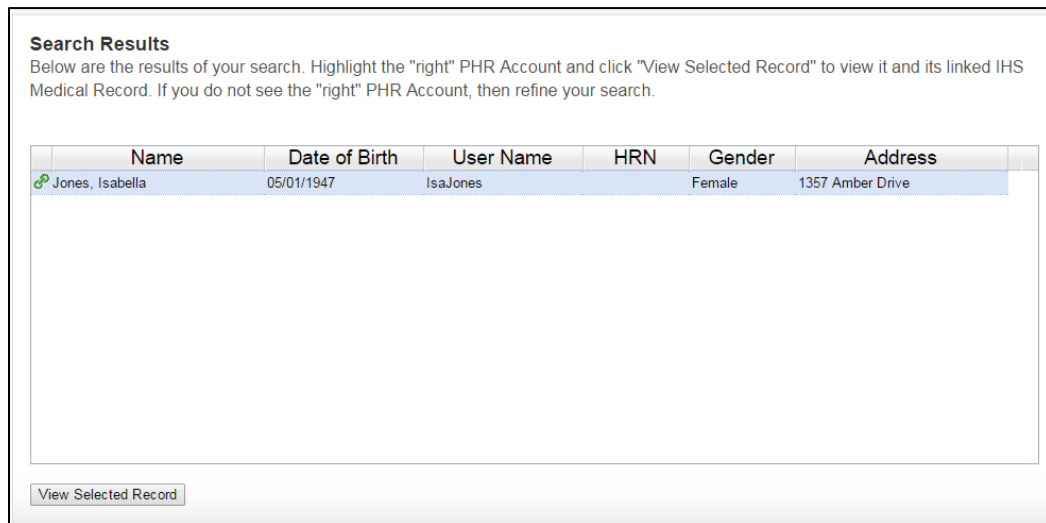
Figure 6-11: Manage Patient – Search Results pane

6.3.2   Link Accounts

The patient's IHS Medical Record must be linked his/her PHR account.

1. Click the link icon (**chain**) next to the patient's name (Figure 6-11). The Process Application - Search results for entered search criterion page opens (Figure 6-12).
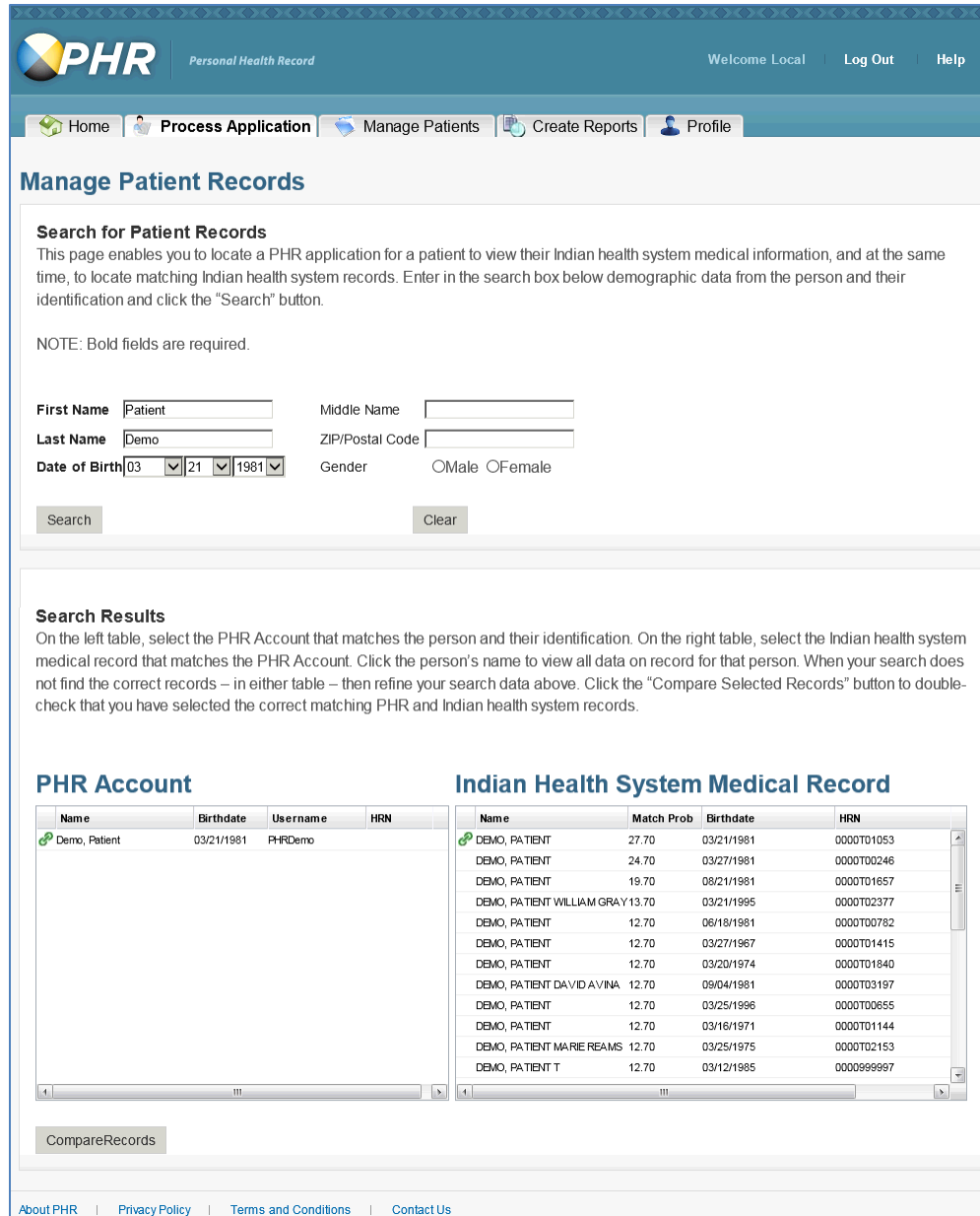
Figure 6-12: Process Application - Search results for entered search criterion

2. Possible warning messages. If you have no warning messages, go to step 3.

    a. When the Registrar searches for the medical record, the PHR queries the IHS
        MPI for results matching the criteria entered. However, because the **IHS MPI**
        data may be extensive, the IHS Medical Record side may time out and not
        return any results. If that happens, a message will display on the IHS Medical
        Record pane indicating a problem with the patient registry (Figure 6-13).

Figure 6-13: Process Application - IHS MPI Search Timeout/Connectivity Error Message

If this message displays, narrow the search results by entering additional search criteria and try searching again. If the error occurs again, please try again later as the PHR may be experiencing connectivity issues with the IHS MPI.

> **Note:** Narrow the search results by entering more specific information in the search criteria fields. Click on any column header to sort that column in ascending order. Click the column header again to sort that column in descending order. You cannot link a patient's PHR account to multiple IHS Medical Records or multiple PHR accounts to one IHS Medical Record. For PHR applications that have already been processed, a chain link icon will display next to the patient's name in the Search Results pane for both the PHR Account and IHS Medical Record.

b. If the search does not return a **PHR Account** for the patient, a message will display on the PHR Account pane indicating that no PHR account was found matching the criteria entered (Figure 6-14).

Figure 6-14: Process Application - No PHR Account Found Message

- Verify the patient is registered to use the PHR as described in Section 6.1.

- If the patient has registered to use the PHR, repeat Steps 3 and 4 by changing some of the search criteria and searching again. For example, the patient may have changed their name; however, the patient registration data may not have been updated in the databases.

- In most cases, changing the search criteria, such as entering a different Last Name, or including the Gender or using the asterisk (*****) symbol in one or more fields, can resolve an issue.

- If an issue is found, it can be corrected by the patient before linking the record

- Have the patient logon to the PHR Patient Web Portal, and follow the instructions in the Section 6.4.1.

c. If the search does not find a matching IHS Medical Record, a message will display on the IHS Medical Record pane indicating that no record was found matching the criteria entered (Figure 6-15).

> ⚠ No Indian health system medical record matches the data you inputted. You may want to adjust the search criteria and search again. If you cannot find a match, then record a non-match.

Figure 6-15: Process Application - No IHS Medical Record Found Message

- If this message displays, narrow the search results by entering additional search criteria and try searching again.

> **Note:** If you continue to receive this message, verify the patient belongs to your facility and that the patient's RPMS health record is active. If the patient's record does not belong to your facility, remind them that his/her facility must have onboarded with the IHS MPI and IHS HIE.

3. To view account details of the search results, do one of the following (Figure 6-12):

a. Double-click the **PHR Account** to view the details of the PHR account's demographic information (Figure 6-16).

- Click the **X** in the upper right corner of the **PHR Account Detail** window to close the window.

Figure 6-16: Process Application - Search Results: PHR Account Detail window

    b. Double-click the **IHS Medical Record** to view the details of the medical record's demographic information (Figure 6-17).

- Click the **X** in the upper right corner of the **IHS Medical Record Detail** window to close the window.

Figure 6-17: Process Application - Search Results: IHS Medical Record Detail window

4. (Optional) Sort or modify the search results in the Search Results pane (see Section 2.3)

5. Click the **PHR Account** record that you are processing (Figure 6-12).

6. Then click the matching **IHS Medical Record** for the same record (Figure 6-12).

7. Click **CompareRecords** (Figure 6-18). The **Process Application - Search Results: CompareRecords** page opens (Figure 6-19).

8. To cancel process application, click **Cancel** and click **OK** on the **Confirmation** dialog to return to the Process Application page.

Note:	*If you cannot locate a matching IHS Medical Record, you must stop processing the patient's application.* If the patient's record belongs to your facility, verify the patient's RPMS health record is active. If the patient's record does not belong to your facility, ask the patient to visit their primary IHS healthcare facility to have their PHR application processed.
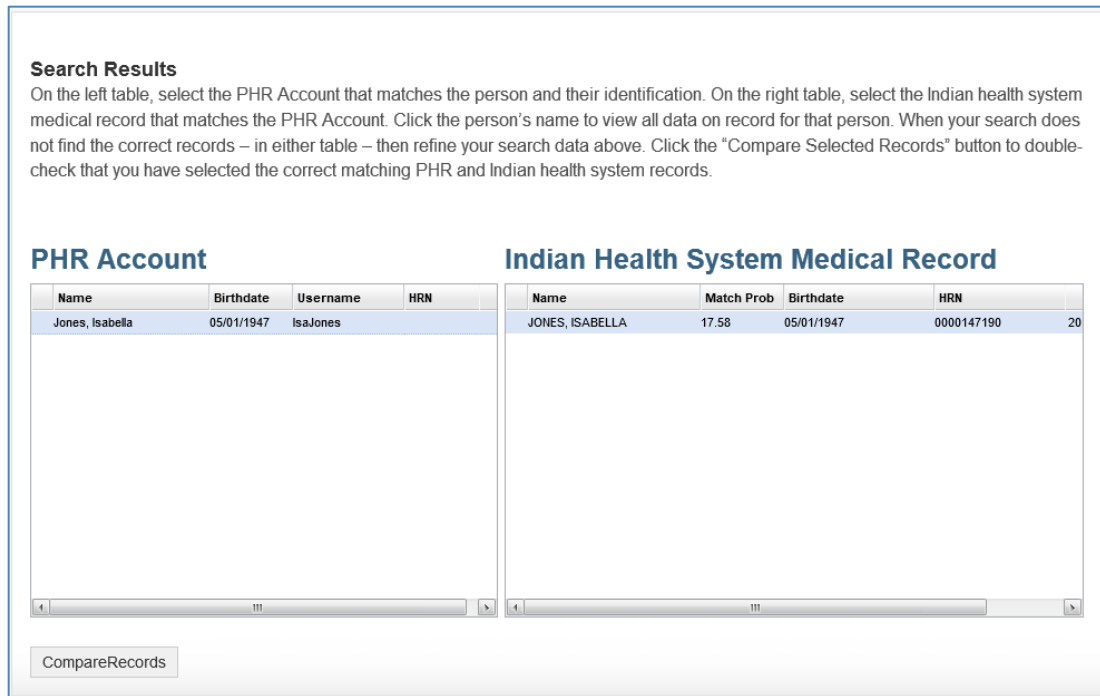
Figure 6-18: Process Application - Search Results: CompareRecords

> **Note:** In most cases, the required search criteria will return one PHR Account and the first returned IHS Medical Record will be the result with the highest probability match. However, you must still review and compare each of the selected records.

9. Compare and confirm that the PHR account and IHS Medical Record match (Figure 6-19).

> **Note:** The IHS Medical Record pane includes HRN and Facility information found during the search to help you confirm patient information. If more than one HRN and facility are listed, they align with each other. For example, the first HRN listed is the HRN found with the first facility listed. The second HRN with the second facility, and so on. These fields can assist in identification and verification process.

Figure 6-19: Process Application - Compare and Confirm Match

a. If the records match **choose** the **Type of Person Verified** and the
   Verification Method (choose the appropriate selection; Figure 6-20).

> **Note:** Although other options exist in the **Type of Person
> Verified** dropdown menu, the Patient option should always
> be selected.

b. Click the **Link** button.
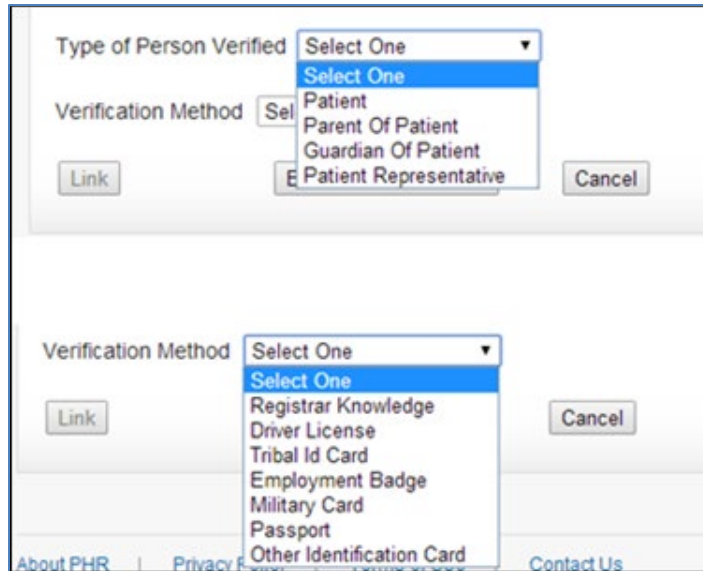
Figure 6-20: Process Application – Type of Person Verified and Verification Method

    c. If the records do not match, do one of the following:

- Click **BackToSearchResults** to return to the Process Application page and repeat your search.

- Click **Cancel** to return to the Process Application page.

10. To complete the linking of the records, do the following:

    a. Click **Yes** on the **Confirm Link** dialog (Figure 6-21) and click **OK** on the **Link Complete** dialog (Figure 6-22).

    b. To cancel the linking of the records, click **No** to return to the Compare and Confirm Match page.
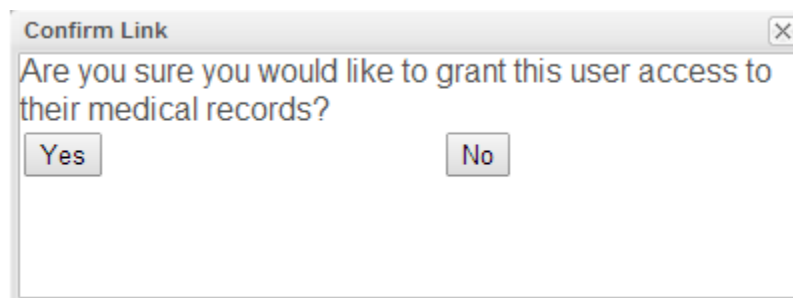
Figure 6-21: Process Application – Link Records: Confirm Link Dialog

Figure 6-22: Process Application – Link Records: Link Complete Dialog

11. Possible warning messages.

    a. **PHR accounts cannot be linked to more than one IHS Medical Record**. If a PHR account is already linked to an IHS Medical Record, the PHR Registrar will see a waring message (Figure 6-23) when comparing records. In this use case, you can only do one of the following:

        • Click **BackToSearchResults** to return to the Process Application page and repeat your search.

        • Click **Cancel** to return to the Process Application page.

Figure 6-23: The Selected PHR Account is already linked to another IHS Medical Record Warning Message

    b. The reverse is also true. **An IHS Medical Record cannot be linked to more than one PHR account**. If an IHS Medical Record is already linked to a PHR account, the PHR Registrar will see a warning message (Figure 6-24) when comparing records. In this use case, you can only do one of the following:

        • Click **BackToSearchResults** to return to the Process Application page and repeat your search.

        • Click **Cancel** to return to the Process Application page.

Figure 6-24: The Selected IHS Medical Record is already linked to another PHR Account Warning Message

   c. If the selected PHR account and the selected IHS Medical Record are linked to each other currently, the PHR Registrar will see a warning message (Figure 6-25) when comparing records. In this use case, you can only do one of the following:

- Click **BackToSearchResults** to return to the Process Application page and repeat your search.

- Click **Cancel** to return to the Process Application page.

> The selected PHR Account is already linked to the selected IHS Medical Record.
> ⊖ PHR cannot link more than one PHR Account to an IHS Medical Record. You may
> want to double-check account and patient information.

Figure 6-25: The Selected PHR Account is already linked to another IHS Medical Record Warning Message

6.4 Process Application: Step 4: Verify Patient Access

After completing the steps is Sections 6.1 through 6.3, the patient's PHR application has been processed as a registered PHR user and the patient can view their IHS health information from their PHR. Before the patient leaves the facility, verify that the patient can do the following:

- Access their PHR.

- View their health information

- View the PHR User Manual (Help).

  – Review and any PHR training materials such as PHR fliers, benefits, features, demos, and other training materials created by your SU/FA.

> **Note:** Patients can view their IHS health information from each Service Unit/Facility in which they are an active patient, if the Service Unit/Facility has on-boarded with the IHS MPI and IHS HIE. It is unnecessary for the patient to visit each Service Unit/Facility where they are an active IHS patient.

6.4.1 Access and Information Verification

1. Go to the PHR Patient Web Portal website at https://phr.ihs.gov (Figure 6-26).

2. Ask the patient to logon to the PHR Patient Web Portal by entering his/her PHR **Username** and **Password** and click **Login**.

> **Note:** If the patient sees the **Next Steps** page (Figure 6-8), verify the patient's PHR Account was successfully linked by repeating **Find Patient Account** in Section 6.3.1. If the account was successfully linked a chain link will display next to the patient's PHR Account. If the patient was successfully linked, verify the patient's PHR Account facility information on the Manage Patients page (Section 7.0). If no facility is listed, the patient may not have an active IHS Medical Record. If the patient belongs to your facility, verify the patient's RPMS health record is active. If the patient's RPMS health record is active, contact help desk. If the patient does not have a record at your facility, unlink the patient's record and ask them to visit their primary facility to have their PHR application processed.

Figure 6-26: PHR Patient Web Portal Logon

3. Verify the patient's health information matches the linked IHS Medical Record by completing the following:

   a. Have the patient **select a facility** (preferably your facility) from the **My Health Records** page (Figure 6-27).
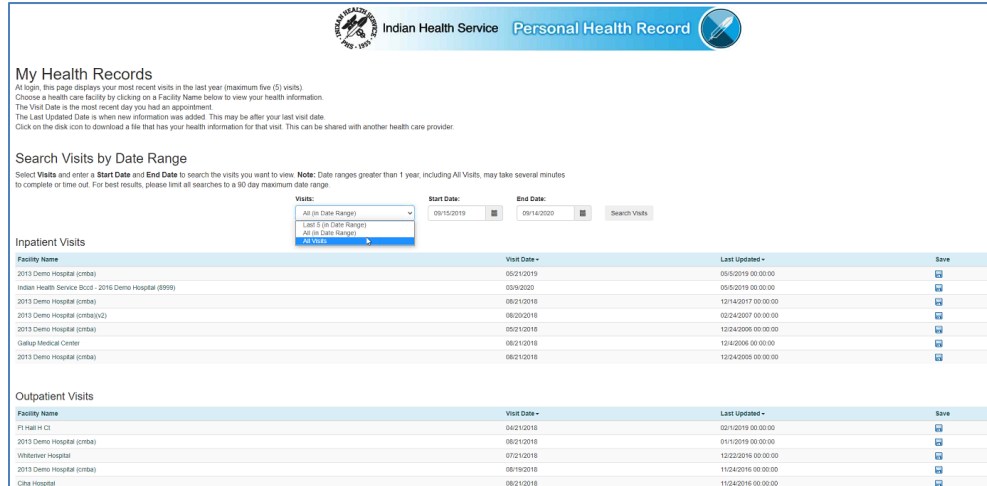
Figure 6-27: PHR Patient Web Portal - My Health Records Page Facility List

- The My Health Records page will only display the last five visits by default. To see all visits, click **All Visits** (Figure 6-27).

b. If the patient does not have any facilities listed on the My Health Records page, verify the patient's facility information on the Manage Patients page (see Section 7.0).

- If the patient's record belongs to your facility, verify the patient's RPMS health record is active.

- If the patient's record is does not belong to your facility, unlink the patient's record, and ask them to visit the facility on the Manage Patients page to have their PHR application processed.

- If the patient was previously given access to someone else's PHR, they will initially see the My Accounts page. Have the patient select the **My Account** link to go to the My Health Records page.

c. Select the **My Info** menu item and verify the patient's demographic information.

Figure 6-28: PHR Patient Web Portal – My Info: About Me Section

- If the demographic information does not match the linked patient's information, unlink the patient records (Section 7.2) and repeat the steps for linking patient records (Section 6.3).

6.4.2   PHR User Manual

Detailed information on how to navigate the PHR Patient Web Portal can be found in the PHR User Manual. After logging into the PHR, patients have access to this manual by selecting the **Help** menu option in the upper right corner of the page.

7.0   Manage Patients

PHR Administrators can view, unlink, and reset PHR User accounts through the Manage Patients page.

7.1   View PHR User Account Information

To view the PHR User account information, do the following:

1. Log on to the PHR Administrator Web Portal application as the PHR **Registrar** as defined in Section 2.0.

2. Click the **Manage Patients** tab (Figure 7-1). The **Search for PHR Patient** page opens (Figure 7-2).

Figure 7-1: Welcome page - PHR Registrar view

Figure 7-2: Manage Patients - Search for PHR Patient pane

3. **Search** for the patient's account to view in the **Search for PHR Patients** page (Figure 7-2) by entering one or more of the following:

   - First Name

   - Last Name

   - Date of Birth

   - PHR Username

   - Middle Name

   - Zip/Postal Code

   - Gender

   - HRN

Note:	Gender requires information in one or more of the other demographic fields. The asterisk (*****) symbol can be used as a wildcard. More data entered in the Search for PHR Patients pane gives a better match.

4. Click **Search** to return the matching results (Figure 7-3). The **Search Results** pane opens (Figure 7-4).

   - Click **Clear** to clear the search fields.
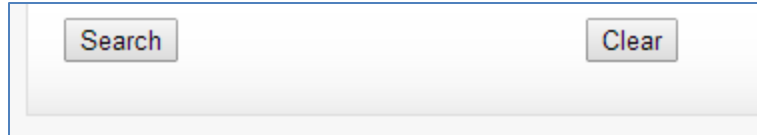
Figure 7-3: Manage Patients – Search and Clear Buttons

5. The search results will be displayed below the Search for PHR Patients pane in the **Search Results** pane (Figure 7-4).

Figure 7-4: Manage Patients - Search results for Last Name: Demo

    a. If the search results do not return a PHR Account for the patient, verify the patient registered to use the PHR as described in Section 6.1.

b. If the patient is registered to use the PHR, repeat Steps 3 and 4 entering only the PHR Username.

c. Verify the patient's information and repeat Steps 3 and 4 by entering as many fields as possible without the PHR Username and search again.

> **Note:** Click on any column header to sort that column in ascending order. Click the column header again to sort that column in descending order.

6. (Optional) Sort or modify the search results in the Search Results pane (see Section 2.3)

7. **Select** a PHR User account to view and click **View Selected Record**. The **Detailed Patient Profile** page opens (Figure 7-5).
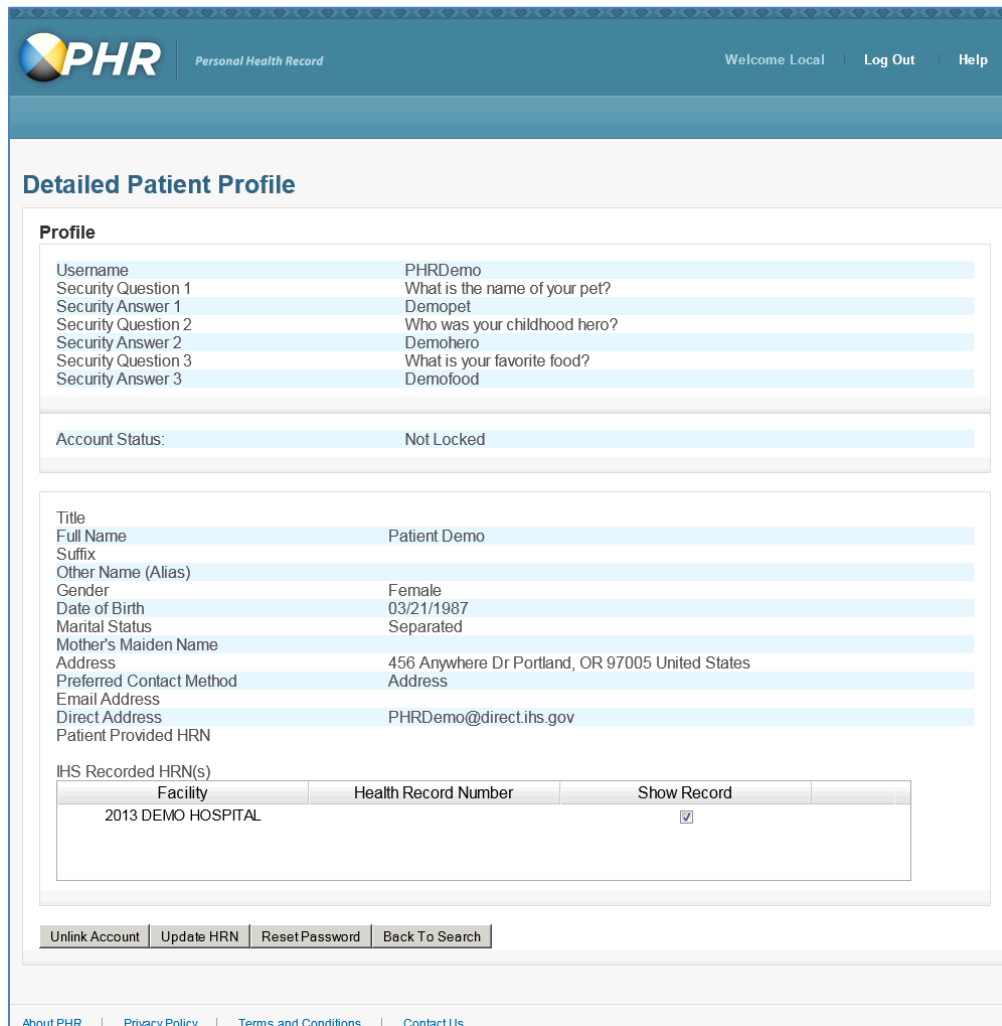
Figure 7-5: Manage Patients – Detailed Patient Profile

8. On the **Detailed Patient Profile** (Figure 7-5) page do one of the following:

   a. Unlink PHR User accounts with their IHS Medical Record by clicking **Unlink Account** (see Section 7.2).

   b. Reset the PHR User's password by clicking **Reset Password** (see Section 7.3)

   c. To update the PHR User's IHS Recorded HRNs section, click **Update HRN** (see Section 7.4)

   d. Update a minor PHR User's emancipated status by clicking **Emancipated Minor**.

   > **Note:** The Emancipated Minor Status and Emancipated Minor button will only display if the PHR user is under the age of 18 (see Section 10.4).

   e. To go the **Manage Patients** page and search for another patient, click **Back** to Search.

   > **Note:** If viewing PHR Account information of a patient whose application has not been processed (see Section 6.0), the IHS Recorded HRNs field will display **No IHS Recorded Health Record Numbers**. If the PHR Account has multiple IHS Medical Records in the IHS MPI and IHS HIE when the PHR application is processed, each facility and HRN will be displayed in the field and the Show Record check box will be checked by default.

7.2   Unlink PHR User Account

In some cases, PHR administrators may need to unlink the PHR User account from their IHS Medical Record. As a result, each PHR administrator can unlink PHR User accounts regardless of their role. These cases include the following:

- PHR Account was accidently mapped to another patient's IHS Medical Record.

- The PHR User requests to terminate the use of their PHR.

- The parent, legal guardian, or court appointed guardian of a minor request to terminate the minor's PHR.

- The minor becomes emancipated and requests to terminate the use of their PHR.

- The legal guardian of an elderly patient or patients living with mental illness requests to terminate the patient's PHR.

To unlink a PHR User account from their IHS Medical Record:

1. Complete Steps 1 through 7 in Section 7.1 and click **Unlink Account** (Figure 7-6).

> **Note:** You can only unlink patients whose application has been
> processed and linked to a medical record. The chain link
> icon will display next to the patient's name in the Search
> Results pane.
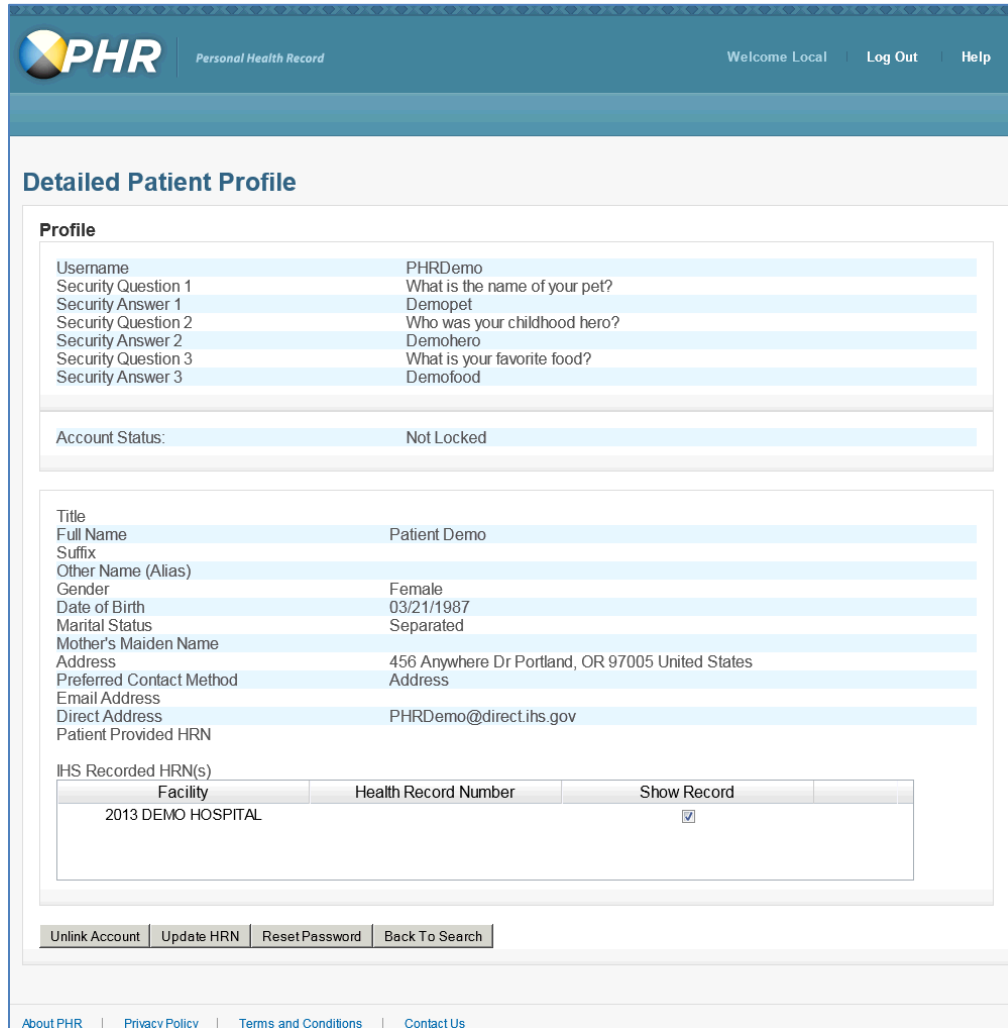
Figure 7-6: Manage Patients - Detailed Patient Profile

2. Verify and confirm the selected account to unlink is the PHR User's account on
   the Unlink PHR & IHS Accounts page.

> **Note:** Before records can be unlinked, the PHR will verify the
> IHS Medical Record by querying the IHS MPI database for
> an update.

a. If the PHR is experiencing issues querying the IHS MPI database, a warning message (Figure 7-7) will display at the top of the Unlink PHR & IHS Accounts page. Please try again later. If the problem persists, see Section 12.0 for reporting the issue.

⊘ Problems with PHR, Try again later.

Figure 7-7: Unlink PHR & IHS Accounts - Problem with the PHR message

b. If the IHS MPI query does not locate the linked record, an error message (Figure 7-8) will display in the Name field on the IHS Medical Record side of the Unlink PHR & IHS Accounts page. In most cases, this message displays because multiple IHS MPI records were merged or unmerged after processing the original PHR application (see Section 6.0). Continue with the unlinking process.

Unlink PHR & IHS Accounts

Confirm that you have selected the "right" account and enter into the text box, "Reason for unlinking the PHR Account from the IHS Medical Record" the reason you are unlinking the selected PHR Account from this IHS Medical Record. Then click the "Unlink" button.

Type of Person Verified:	Patient
Verification Method:	DriverLicense
Verified On:	11/26/2018

PHR Account		**Indian Health System Medical Record**	
Name:	Demo, Patient	Name:	Error, Linked Record Not Found
HRN:		HRN:	
Gender:	Female		

Figure 7-8: Unlink PHR & IHS Accounts - Error, Linked Record Not Found message

3. Enter the reason for unlinking the account in the **Reason for unlinking the PHR Account** text box (Figure 7-9).

Figure 7-9: Manage Patients: Unlink PHR & IHS Accounts

4. To continue unlinking the PHR User account, click **Unlink** on the **Unlink PHR & IHS Accounts** page (Figure 7-9). The **Confirm Unlink** dialog opens (Figure 7-10).

    a. To cancel unlinking the PHR User account, click **Back** to Search to return to the Manage Patients page.

5. Click **Yes** on the **Confirm Unlink** dialog (Figure 7-10).The Unlink Confirmation page opens.

    a. To cancel the unlinking of the records, click **No** to return to the Unlink PHR & IHS Accounts page.

Figure 7-10: Manage Patients: Confirm Unlink dialog

6. The **Unlink Confirmation** page (Figure 7-11) has a **Go To Search** button and a **Go Home** button. Click the appropriate button.
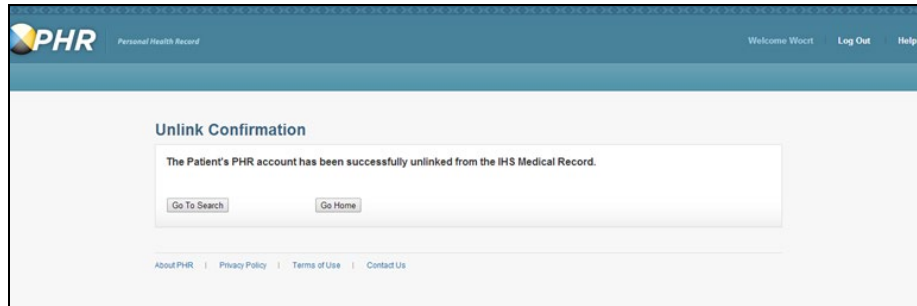
Figure 7-11: Manage Patients: Unlink Confirmation

7. Verify that unlinking was successful. Go to the PHR Patient Web Portal website at https://phr.ihs.gov (Figure 7-12).

Figure 7-12: PHR Patient Web Portal Logon

8. Ask the patient to logon to the PHR Patient Web Portal by entering their PHR Username and Password, and click **Login**.

9. Verify the patient cannot view their health information. If unlinking was successful, the PHR Patient Web Portal application displays **The Next Steps** page (Figure 7-13).
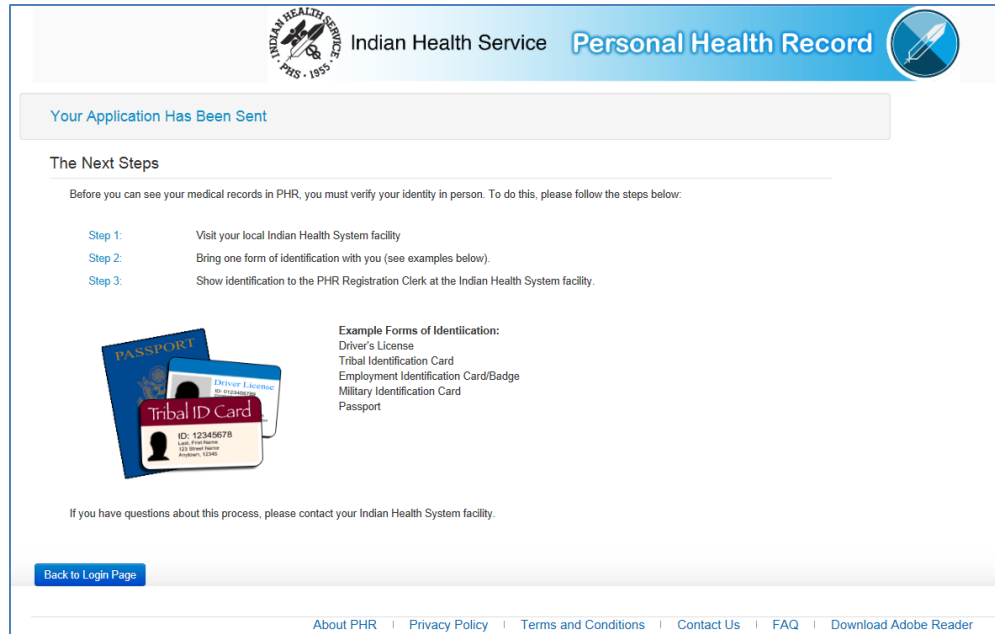
Figure 7-13: PHR Patient Web Portal application Next Steps

7.3   Disable PHR User Account

To disable a PHR User account, repeat the steps in Section 7.2.

7.4   Update HRN Facility List

In some cases, PHR Administrators may not see their Service Unit/Facility listed in the IHS Recorded HRNs Section of the Manage Patient Detailed Patient Profile page. If any of following cases apply, the HRN must be updated.

- Patient was linked to a record in which he or she has multiple IHS Medical Records in the IHS MPI.

- Patient is new to the facility.

- Patient was first seen at the facility after the patient's PHR application was processed as defined in Section 6.0.

- Multiple IHS MPI records were merged into one IHS MPI record after the patient's PHR application was processed as defined in Section 6.0.

To update the IHS Recorded HRNs Section of the Manage Patient Detailed Patient Profile page, do the following:

1. Complete Steps 1 through 7 in Section 7.1 and click **Update HRN** (Figure 7-5). The Manage Patient Profile (Update HRN) dialog opens.

> **Note:** Before the facility list can be updated, the PHR will verify
> the IHS Medical Record by querying the IHS MPI database
> for an update.

   a. If an IHS MPI record is not found, a dialog will display indicating a linked
      record could not be found, and asks if you want to unlink the account.

   • This message will only display if multiple IHS MPI records were merged
     or unmerged after processing the original PHR application (see
     Section 6.0) or the PHR is experiencing issues querying the IHS MPI.
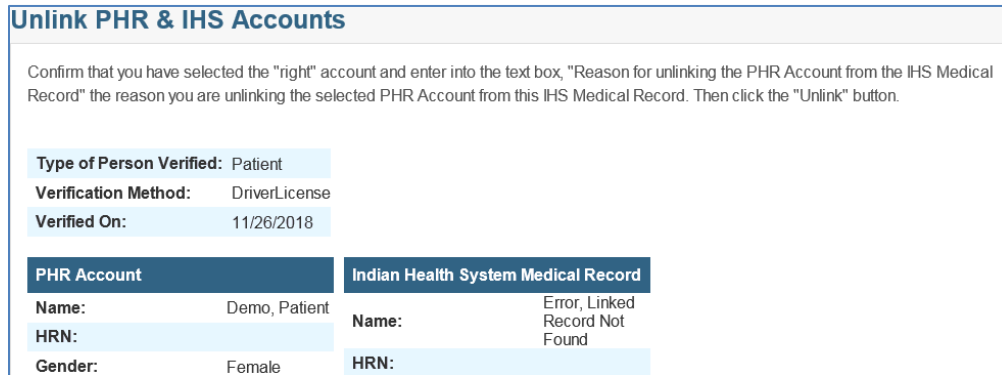
2. To continue, click **OK** on the **Manage Patient Profile (Update HRN)**.
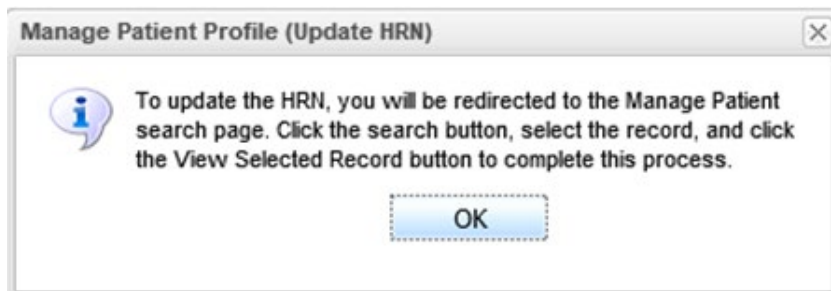
Figure 7-14: Manage Patient Profile (Update HRN) dialog

> **Note:** Although an IHS MPI record could not be found for the
> linked account, it is recommended that you click **No** and
> search for the patient record as described in Section 6.3 to
> make sure the PHR is not experiencing issues querying the
> IHS MPI. If a matching IHS Medical Record is found from
> that query, proceed with the unlinking processes as
> described Section 7.2. A PHR record should not be
> unlinked except as described in Section 7.2.

   a. To return to the Manage Patient Detailed Patient Profile page, click **No**.
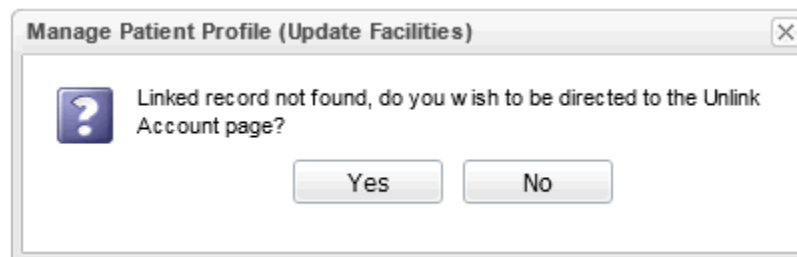
Figure 7-15: Manage Patient Profile (Update Facilities) dialog

3. Click **OK** on the **Manage Patient Profiles (Update Facilities)** dialog.
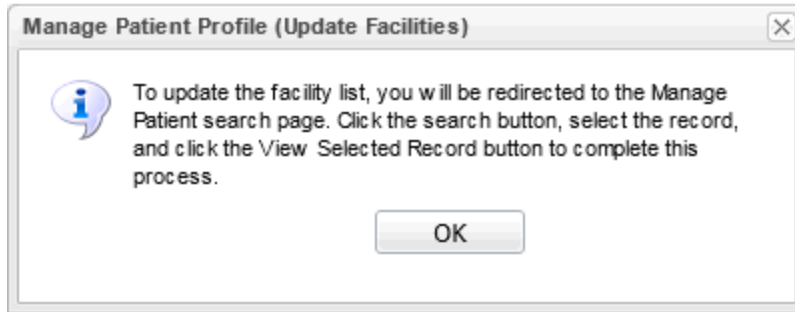
Figure 7-16: Manage Patient Profiles (Update Facilities) dialog

> **Note:** A new call to the IHS MPI is needed to update or refresh the patient facility list. As a result, clicking the **OK** button will redirect to the Admin user to the Manage Patients page, which will invoke the call to the IHS MPI.

4. On the Manage Patients search page, leave the search settings as is and click **Search**.

5. Select the PHR user account from the returned search results and then click **View Selected Record**.

6. If the PHR user account has an updated IHS MPI record, the IHS Recorded HRNs Section of the Detail Patient Profile page will be updated to include additional facilities.
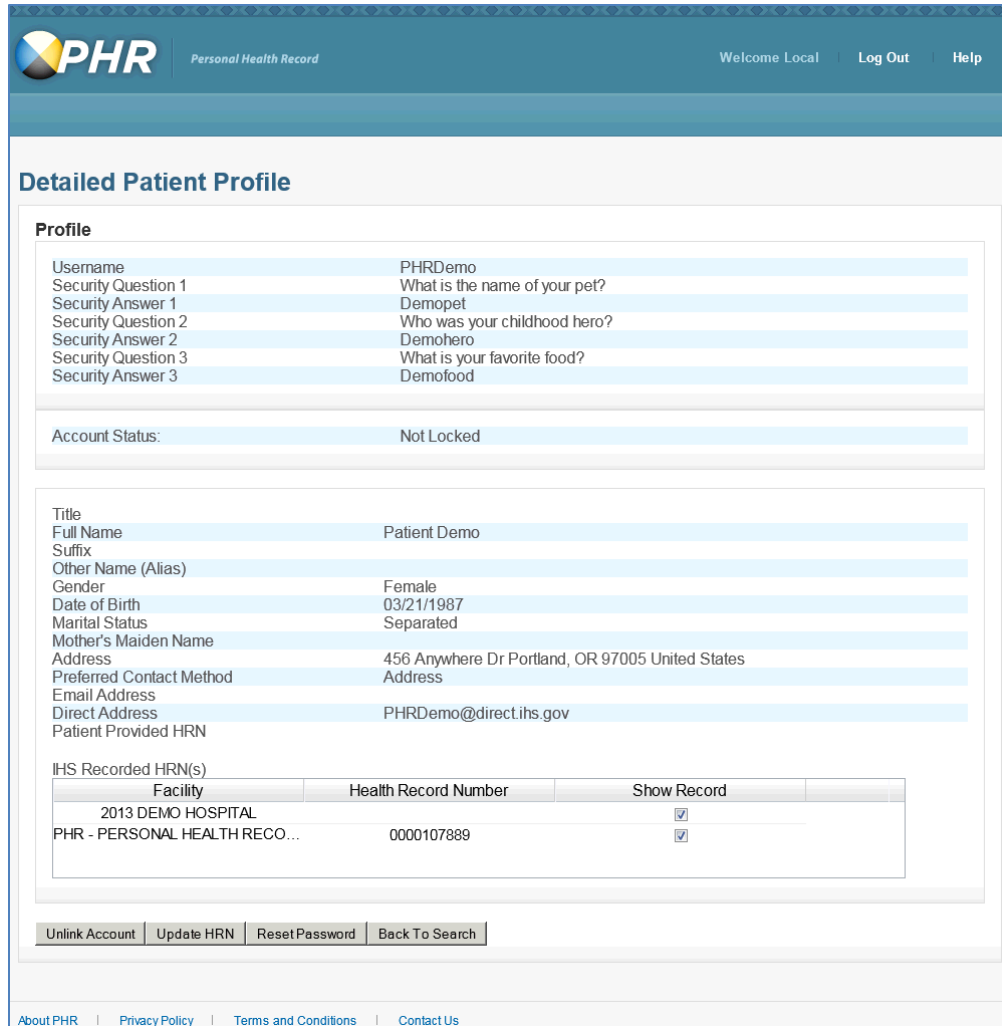
Figure 7-17: Manage Patients - Detailed Patient Profile

7.5   Hide Selected Facility Visit Documents

In some cases, PHR patient users may request not to see visit documents from specific facilities. This may happen because of one or more of the following:

- Patient was last seen at the facility several years ago, and the patient believes the visit data is no longer relevant.

- Patient has relocated and no longer visits a particular facility.

- Patient does not want to see visits from a specific facility.

To hide visit documents for a specific facility from the patient's PHR:

1. Complete Steps 1 through 7 in Section 7.1.

2. In the **IHS Recorded HRN(s)** Section of the **Detail Patient Profile** page (Figure 7-18), **uncheck** the **Show Record** check box for any facility for which the PHR patient user does not want to see visit documents. Click **Update HRN**.

> **Note:** The **Show Record** check box must be checked for at least one facility.
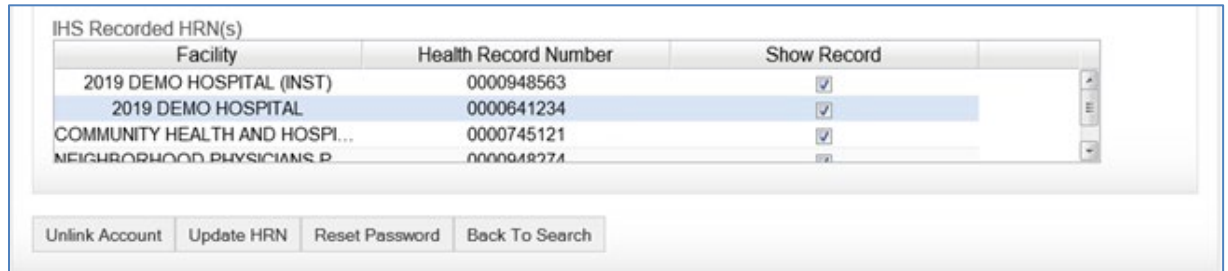
Figure 7-18: Manage Patients - Detailed Patient Profile

3. Click **OK** on the **Manage Patient Profiles (Update Facilities)** dialog (Figure 7-19). Clicking **OK** redirects you to the search page (Figure 7-4).

> **Note:** A database update is needed to update or refresh the patient facility list. As a result, clicking the **OK** button will redirect to the Admin user to the **Manage Patients** page, which will invoke the call to the IHS MPI to check for new facilities and update the database to show or not show records.
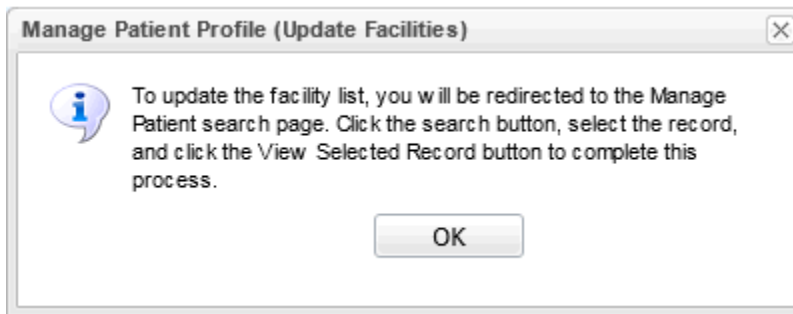
Figure 7-19: Manage Patient Profiles (Update Facilities) dialog

> **Note:** If the PHR patient user does not want to see any facility visit information, verify that the patient wishes to disable their PHR and follow the steps in **Unlink PHR User Account** (Section 7.2) to unlink their PHR.

4. Verify the update. On the **Manage Patients Search Results** page (Figure 7-4), leave the search settings as is and click **Search**.

5. Select the PHR user account from the returned search results and then click **View Selected Record**.

6. Verify that the IHS **Recorded HRN(s)** Section of the **Detail Patient Profile** page (Figure 7-20) has been updated and shows the facilities with **Show Record** check box changes performed in step 2.

> **Note:** For any new facilities added to this section, the **Show Record** box will be checked by default.
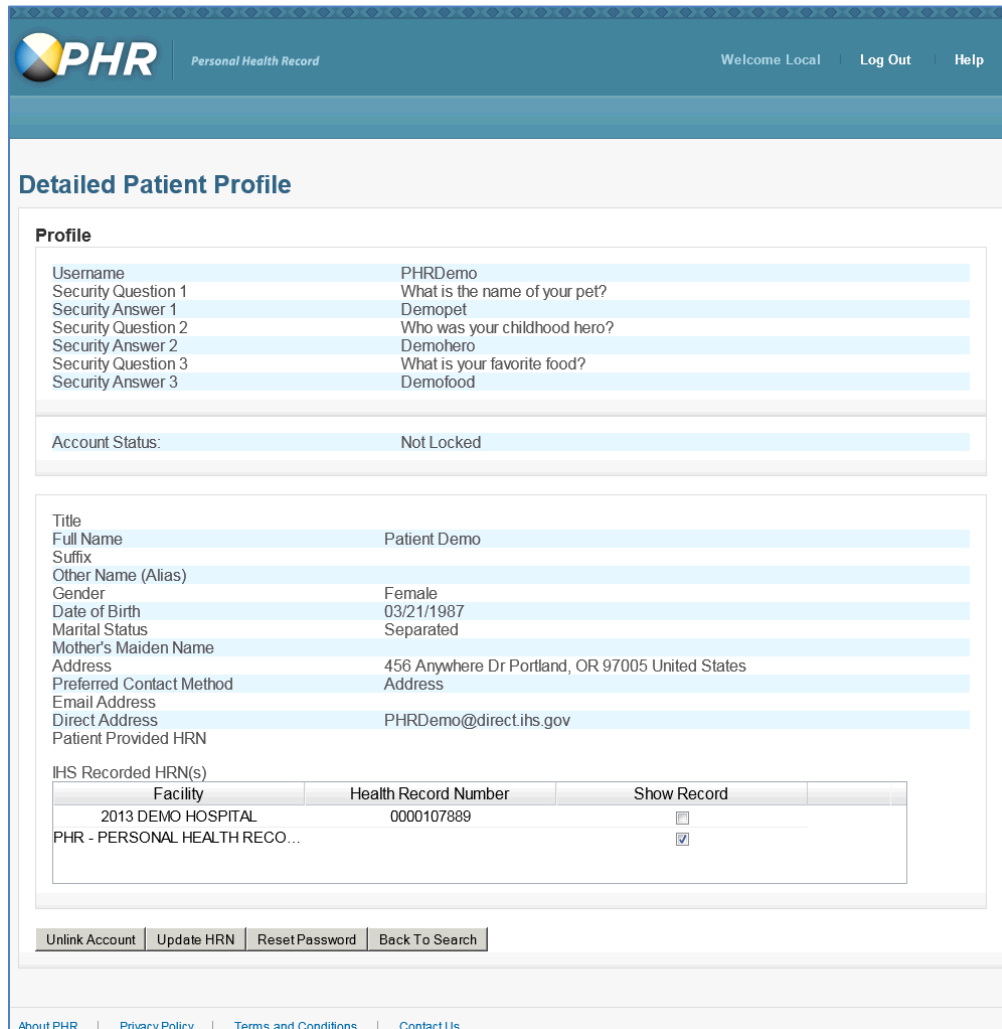
Figure 7-20: Manage Patients - Detailed Patient Profile

7. Verify the facility visit documentation does not display in the PHR patient user's PHR.

   a. Go to the PHR Patient Web Portal website at https://phr.ihs.gov.

      b. Ask the patient to logon by entering their PHR Username and Password and clicking Login.

      c. Verify they no longer see documents from the removed facilities.

7.6   Show Hidden Facility Visit Documents

PHR patient users may request to have visit documents from specific facilities that were previously hidden to be visible in their PHR. To show previously hidden facility documents, do the following:

1. Complete Steps 1 through 7 in Section 7.1.

2. In the IHS **Recorded HRN(s)** Section of the Detail Patient Profile page, **check** the **Show Record** check box for any facility previously hidden. Click **Update HRN**.

3. Complete Steps 3 through 7 in Section 7.5.

7.7   Reset PHR Patient User Account Password

Even though the PHR Patient Web Portal allows PHR Users to reset their password online, PHR administrators may be asked by the PHR patient user to reset their password. Each PHR administrator, regardless of their role, can reset PHR patient user account passwords. Reasons for resetting are the following:

- The PHR patient user forgot the answers to their security questions.

> **Note:** The PHR Patient Web Portal allows PHR patient users to recover their PHR Username online. See the PHR User Manual for more details. Administrators resetting PHR patient user account passwords must verify the identity of the PHR patient user requesting the password reset. In-person verification is preferred and defined in Section 6.2. If in-person verification is not possible, a series of questions can be asked to establish identity or follow HIPAA and/or facility procedures for establishing identity.

To reset a PHR User account password, do the following:

1. Complete Steps 1 through 7 in Section 7.1 and click **Reset Password**. The Reset Password for Patient Account page (Figure 7-21) opens.
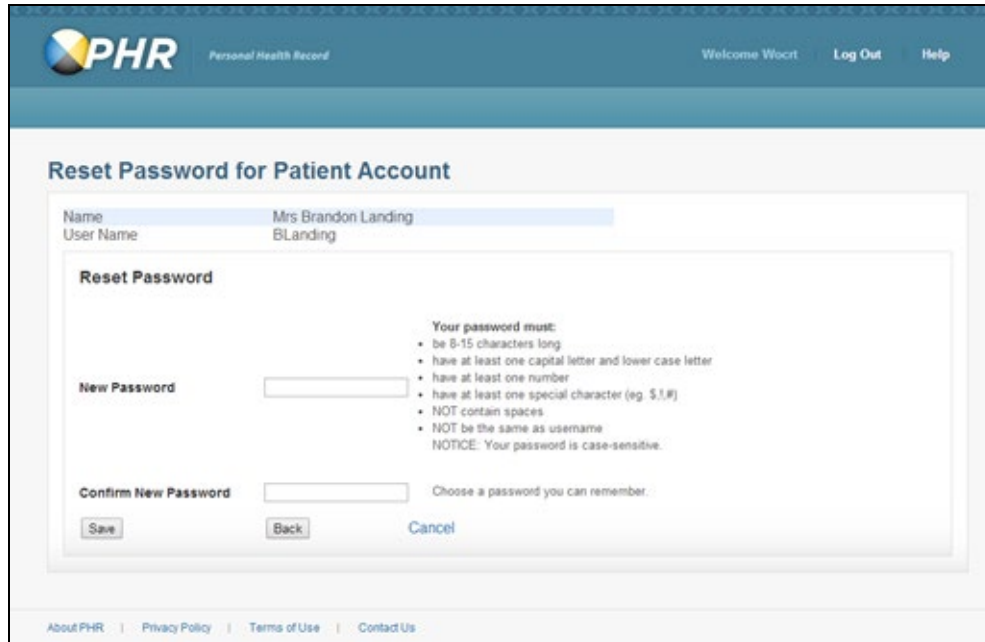
Figure 7-21: Manage Patients – Reset Password for Patient Account

2. **Type** a new password in the **New Password** text field (Figure 7-21).

> **Note:** Follow the instructions on the page to ensure the new password meets the password requirements.

3. **Type** the new password again in the **Confirm New Password** text field and do one of the following:

   a. To save the new password, click **Save** (Figure 7-21). The Confirm Patient Account Updated page opens (Figure 7-23).

   b. To return to the Detailed Patient Profile page, click **Back** (Figure 7-21).

   c. To cancel the password reset, click the **Cancel** link and do one of the following on the **Cancel Password Reset dialog** (Figure 7-22):

      - Click **OK** to return to the Manage Patients page.

      - Click **Cancel** to return to the Reset Password for Patient Account page.
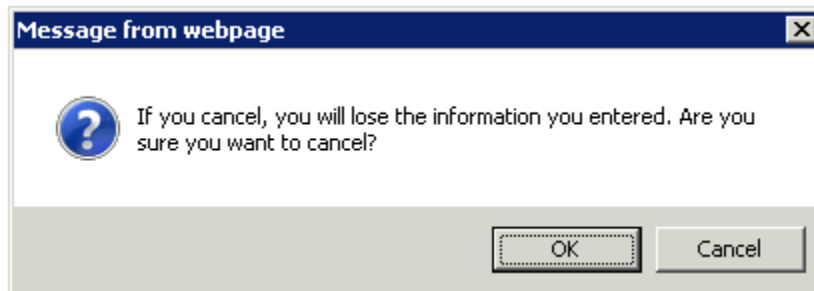
Figure 7-22: Manage Patients: Cancel Password Reset dialog

4. On the **Confirm Patient Account Updated** page (Figure 7-23), do one of the following:

    a. Give the PHR patient user their new password information verbally.

    b. Print the Confirm Patient Account Updated page by clicking **Print** and give the printed page to the PHR patient user.

    c. To go back to the Manage Patients page, click **Back to Manage Patients**.
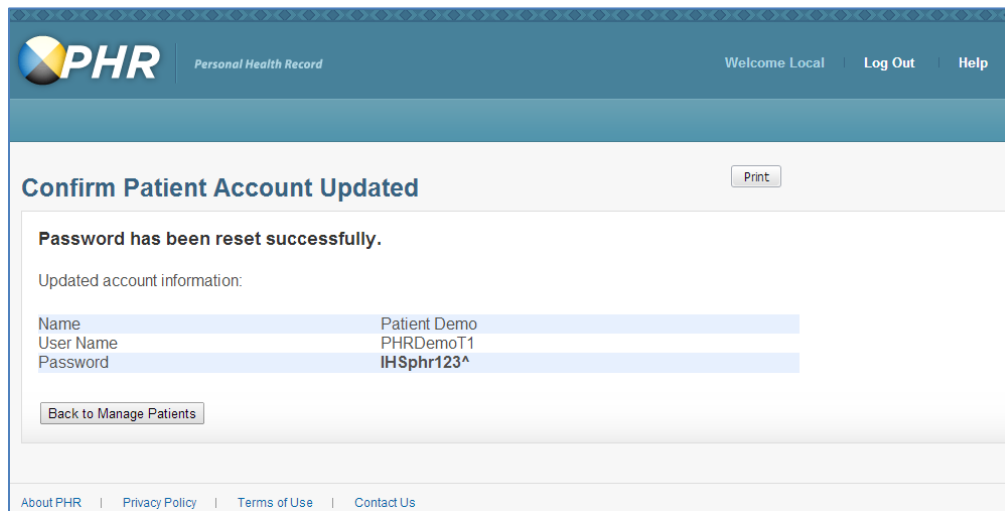
Figure 7-23: Manage Patients: Password Reset Confirm Patient Account Updated

8.0   Create Reports

The PHR records specific event types that occur within the PHR Administrator and Patient Web Portal applications. PHR Administrators may be asked to generate a report for one or more of these event types for a specific role, a specific PHR administrator, or a specific patient. These requests are for auditing purposes and there may be other requests, such as a patient inquiry regarding their PHR activity. The amount of information returned in a report is as follows:

- **National Administrators** can create a report for the entire PHR system. For example: a report for the Registrar role will return the events generated by every Registrar in the PHR system.

- **AO Administrators** can only create a report within their Area. For example, a report for the Registrar role will only return the events generated by a Registrar within their AO. This limitation is applied for any Role selected.

- **SU/FAs** can only create a report within their Service Unit/Facility. For example a report for the Registrar role will only return the events created by a Registrar within their Service Unit/Facility. This limitation is applied for any Role selected.

- **Registrars** can only create a report within their Service Unit/Facility. For example a report for the Registrar role will only return the events created by a Registrar within their Service Unit/Facility. This limitation is applied for any Role selected.

- **Patient**: This role is available to all PHR Administrators, regardless of their role and will display events created by PHR users (patients).

- The report results contain the following information about each event selected:
    - Username
    - IP Address
    - Last Name
    - First Name
    - Event Type
    - Severity
    - Message
    - Time Stamp

To create a report for a PHR event, do the following:

1. Logon to the PHR Administrator Web Portal application as defined in Section 2.0. The Welcome page for PHR Administrators opens (Registrar page is shown in Figure 2-2).

2. Click the **Create Reports** tab. The **Create Reports** page opens. Each type of administrator will have different options on this page. (Figure 8-1: Create Reports page for National Administrators; Figure 8-2: Create Reports page for AO Administrators; Figure 8-3: Create Reports page for SU/FA Administrators; Figure 8-4: Create Reports page for PHR Registrars)

3. On the **Create Reports** page, select a **Role** from the in the **Specify Report Data** pane.

> **Note:** A PHR **role** and date range must be selected to generate a report. PHR Administrators will only see the roles for which they can create a report. Once a role is selected, the Event Type field will be populated. For more details on recorded event types, see Appendix A.

Figure 8-1: Create Reports page for National Administrators

Figure 8-2: Create Reports page for AO Administrators

Figure 8-3: Create Reports page for SU/FA Administrators

Figure 8-4: Create Reports page for PHR Registrars

4. On the **Create Reports** page, **select** an Event Type (Figure 8-5).

> **Note:** To run a report for multiple event types, select an event type, hold the Alt key and select additional event types until you have selected all the events you want in the report. If you do not select an event, the report will run for all events.

Figure 8-5: Create Report Page for SU/FA – Specify Report Data: Event Type

5. Enter a date range for the report by entering a **month**, **day**, and **year** for both the **Date From** and Date **To** fields (Figure 8-5).

> **Note:** Based on the date range entered, the report may take several minutes to complete. In some cases, the report may time out. If this happens, reduce the date range and try again. For optimal performance, limit the date range to 90 days.

6. To narrow the report results, enter or **select** one or more of the following in the **Specify Report Data** pane by following the instructions on the page (Figure 8-5):

    a. User Name

    b. First Name

    c. Last Name

    d. Event Type

    e. Severity

> **Note:** The asterisk (*****) symbol can be used as a wildcard to replace zero or more characters in a text field.

7. Click the **Reports Results** to display the results or click **Clear** to clear the fields (Figure 8-5).

8. (Optional) Sort or modify the search results in the **Search Results** pane (see Section 2.4)

9. (Optional) Export and save the report results by selecting the **.csv (Excel file)** option. Click the **Generate Report** link in the **Report Results** pane (Figure 8-6).

Figure 8-6: Create Reports - Report Results for Demo Administrator

9.0 Locked Administrative Accounts

A PHR Administrator who fails to logon to the PHR Administrator Web Portal successfully in five consecutive attempts will be locked out. An administrator whose account has been locked will need to have their password reset by an up-level PHR Administrator. See Section 4.4.

If the account becomes locked, the administrator will receive the message shown in Figure 9-1. Click **OK**.
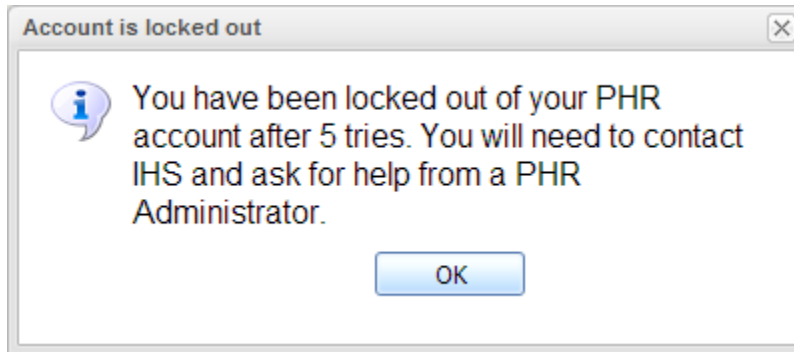
Figure 9-1: Account is locked out dialog

If a PHR Administrator account is locked, the administrator cannot logon and will receive a message on the PHR Administrator Login page (Figure 9-2) informing the administrator that their account is locked.
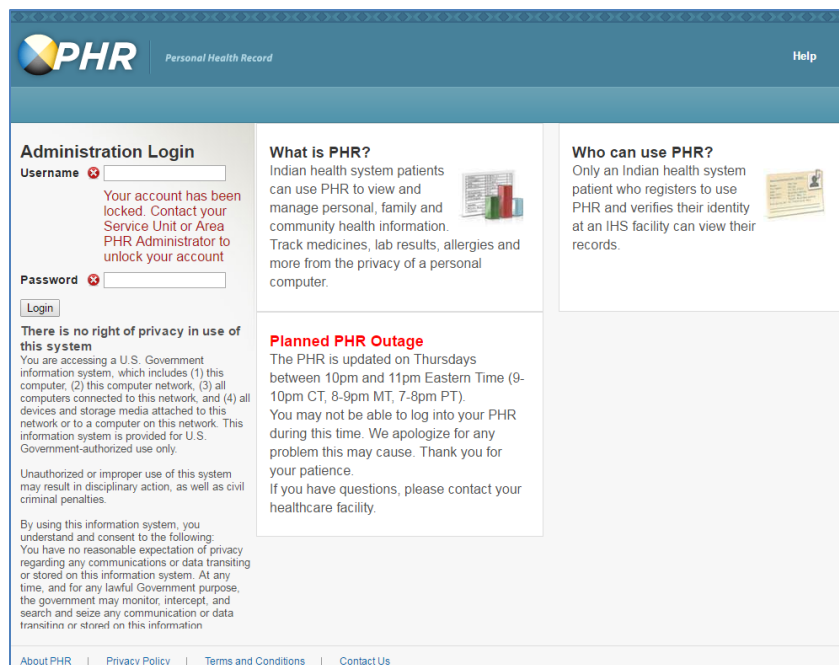
Figure 9-2: PHR Administrator Logon page with your account has been locked message

10.0   Grant Access to a Minor's PHR

A parent, legal guardian, court appointed guardian, or individuals acting *in loco parentis* may request access to a minor's PHR by completing the [IHS-810](https://www.ihs.gov/sites/forpatients/themes/responsive2017/display_objects/documents/patientforms/IHS-810.pdf) form (https://www.ihs.gov/sites/forpatients/themes/responsive2017/display_objects/documents/patientforms/IHS-810.pdf) according to the Service Unit/Facility policies and procedures. Once the form has been approved by the minor's provider or according to the Service Unit/Facility policy and procedures, the **PHR Registrar** will complete the following before granting access to the minor's PHR.

> **Note**: The individual does not have to be an IHS patient to be given access to the minor's PHR; however, the individual listed on the approved IHS-810 form must have a registered PHR account at a minimum.

1. Register the minor to use the PHR as described in Section 6.1.

> **Note:** In some cases, a parent, legal guardian, court appointed guardian, or individuals acting *in loco parentis* may have created the minor's PHR account already. If so, reset the minor's password as described in Section 7.7 and reset the minor's security questions by logging into the minor's PHR Patient Web Portals described in Section 6.1.

2. Record the minor's PHR Username and Password on the IHS-810 form and file the form according to the Service Unit/Facility's policies and procedures.

3. Verify the identity of the individuals listed on the approved IHS-810 form as described in Section 6.2.

4. Link health accounts in the minor's PHR account as described in Section 6.3.

5. Verify that the minor's health information matches the linked IHS Medical Record as described in Section 6.4.

> **Note:** Minors cannot be provided a PHR account at this time. In a future release of RPMS software, the PHR will filter sensitive information from displaying in the minor's PHR account. The information below describing the procedure for registering a minor is for use after the PHR can filter sensitive information. Please contact your PHR administrator if you have any further questions.

10.1   Add Access

To grant access to the individuals listed on the approved IHS-810 form, do the following:

1. Go to the PHR Patient Web Portal website at https://phr.ihs.gov.

2. Logon to the PHR Patient Web Portal by entering the minor's PHR **Username** and **Password** (Figure 6-1).

3. Click the **Manage My Accounts** link in the lower-left of the **My Health Records** page (Figure 10-1). The **My Accounts** page opens (Figure 10-2).

Figure 10-1: PHR Patient Web Portal - My Health Records page

4. Click the **Add/Update Account Access** link on the **My Accounts** page (Figure 10-2). The **Manage Access to my Personal Health Record (PHR)** page opens (Figure 10-3).
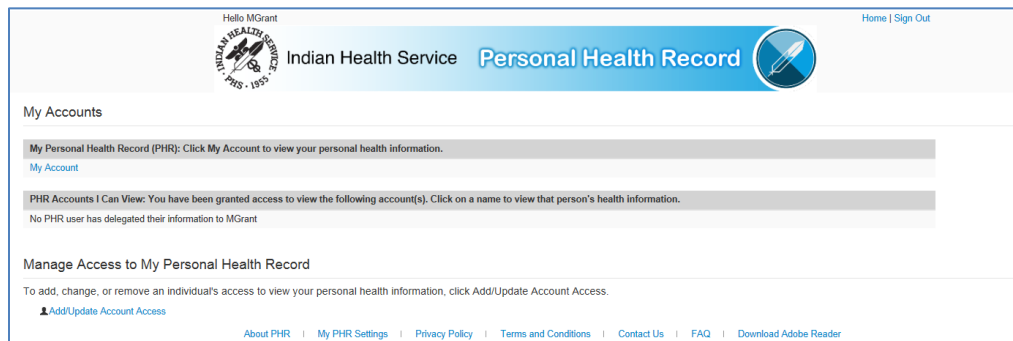
Figure 10-2: PHR Patient Web Portal - My Accounts page

5. Click **Add Access** on the **Manage Access to my Personal Health Record (PHR)** page (Figure 10-3). The **Add Access to your Personal Health Record** opens (Figure 10-4).

Figure 10-3: PHR Patient Web Portal - Manage Access to my Personal Health Record

6. Complete the form on the **Add Access to your Personal Health Record (PHR)** page (Figure 10-4) and click **Verify Username** to continue. The **Personal Health Record (PHR) Access Types page** opens (Figure 10-5).

> **Note:** You must enter the PHR Username, first name, and last name of the individual being granted access to the minor's PHR.

Figure 10-4: PHR Patient Web Portal - Add Access to your Personal Health Record

   a. To cancel and return to the **Manage Access to my Personal Health Record (PHR)** page, click **Cancel**.

7. **Choose** one of the following types of access to grant to the user from the **Type of Access** dropdown menu on the **Personal Health Record (PHR) Access Types** page (Figure 10-5) and select and click **Next** to continue. The Confirm Access: Full Access page opens (Figure 10-6).

- **Full Access** – Selecting this option will allow the user to view all of the patient's personal health information except for the **My Messages** section. The user can also download the patient's visit information.

> **Note:** If the approved IHS-810 form has limitations regarding the data that can be viewed in the minor's PHR, do not select this option.

- **Limited Access** – Selecting this option will allow the user to view only the Section that the patient wants the user to view. Access to the **My Messages** Section is not permitted.

> **Note:** You can change access types and sections anytime on the **Manage Access to My Personal Health Record** page.

Figure 10-5: PHR Patient Web Portal - Personal Health Record (PHR) Access Types

a. To go back to the **Add Access to your Personal Health Record** page, click **Previous**.

b. To cancel and return to the **Manage Access to my Personal Health Record (PHR)** page, click **Cancel**.

8. If you selected the limits access type, go to Step 9. If you selected full access type, do one of the following on the **Confirm Access** page (Figure 10-6):

a. Go back to the **Personal Health Record (PHR) Access Types** page by clicking **Back**.

b. Grant access to the user by clicking **Add Access**.

c. Cancel and return to the **Manage Access to my Personal Health Record (PHR)** page by clicking **Cancel**.

Figure 10-6: PHR Patient Web Portal - Confirm Access: Full Access

9. If you selected the limited access type, do one of the following on the **Personal Health Record (PHR) Section Access** page (Figure 10-7):

   a. Follow the instructions on the screen to select or de-select the PHR sections to grant the user access and click **Next** to continue.

   > **Note:** By default, **the Download My Data Section** is unchecked, which prevents the user from downloading the patient's visit information.

   b. To cancel and return to the **Manage Access to my Personal Health Record (PHR)** page, click **Cancel**.
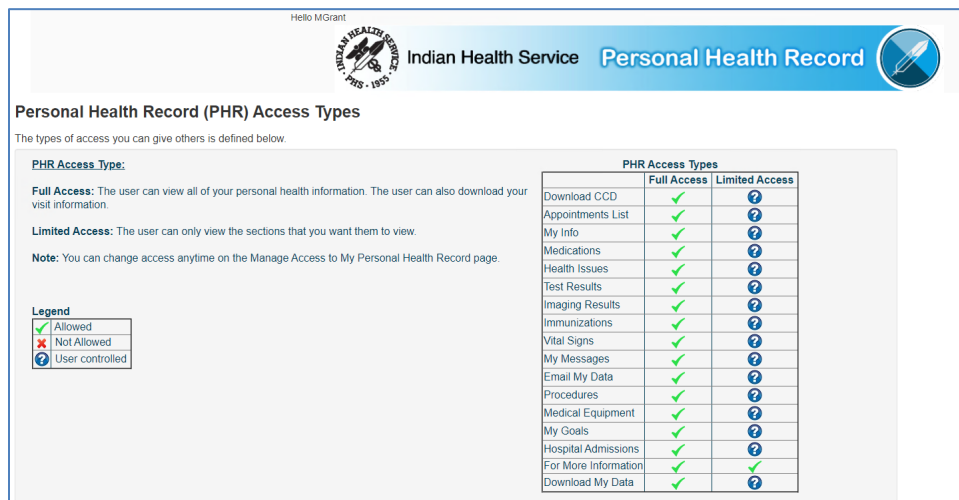
Figure 10-7: PHR Patient Web Portal - Personal Health Record (PHR) Access Types

10. On the **Confirm Access** page (Figure 10-8), do one of the following:

   a. To go back to the **Personal Health Record (PHR) Section Access** page, click **Back**.

b. To grant access to the user, click **Add Access**. The Manage Access to my Personal Health Record (PHR) page opens (Figure 10-9).

c. To cancel and return to the **Manage Access to my Personal Health Record (PHR)** page, click **Cancel**.
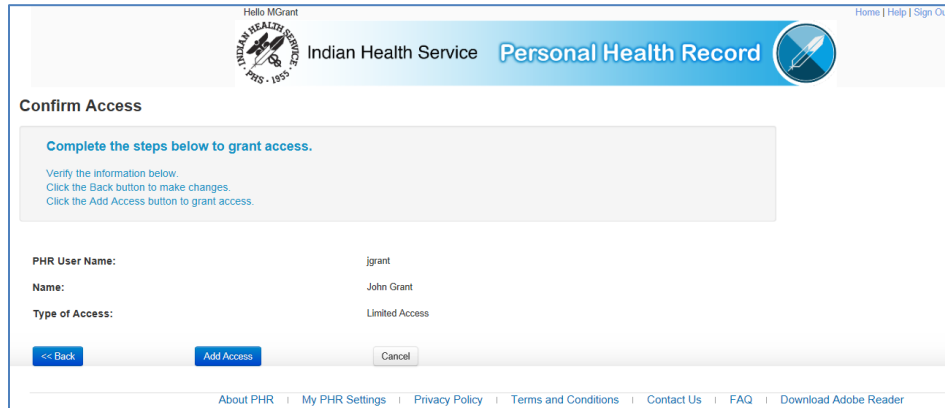
Figure 10-8: PHR Patient Web Portal - Confirm Access : Limited Access

11. On the **Manage Access to my Personal Health Record (PHR)** page (Figure 10-9), verify the user granted access was added to the table.

Figure 10-9: PHR Patient Web Portal - Manage Access to my Personal Health Record with User Access Displayed

12. Log off of the minor's PHR and verify the user given access can view the minor's health information.

a. Have the user given access logon to the PHR using their individual PHR account as in Section 6.1.

b. On the **My Accounts** page (Figure 10-10), click the minor's PHR account under the **PHR Accounts I Can View** section. The My Health Records Page Facility List opens (Figure 10-11).
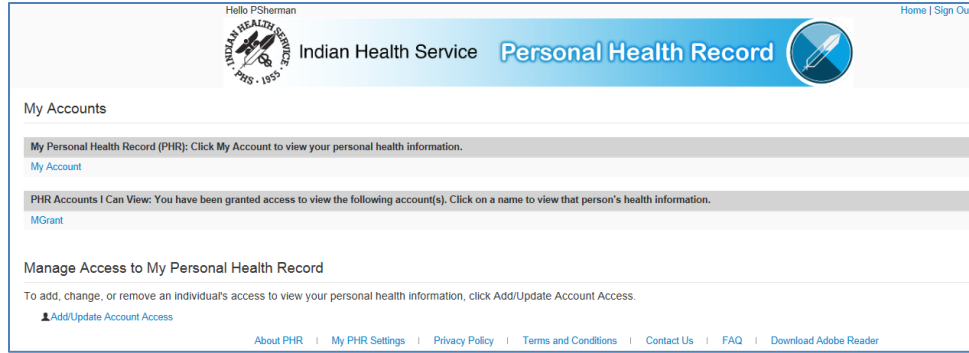
Figure 10-10: PHR Patient Web Portal - My Accounts

c. Select one of their facilities (preferably your facility) from the **My Health Records** page (Figure 10-11). My Info: About Me section opens (Figure 10-12).
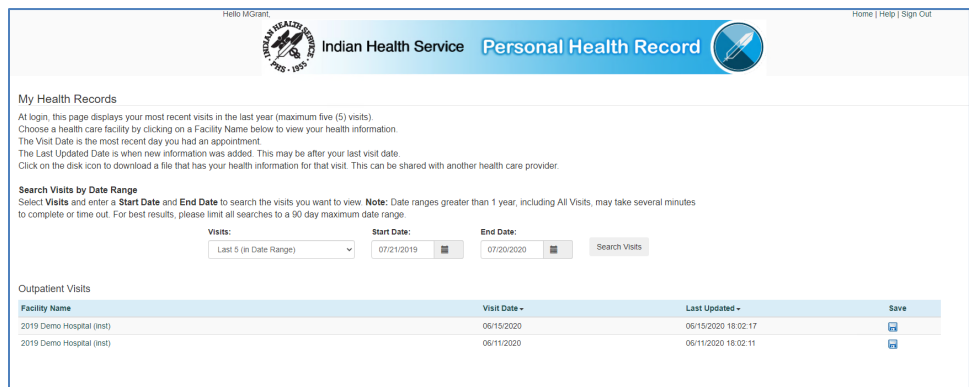
Figure 10-11: PHR Patient Web Portal - My Health Records Page Facility List

d. Select the **My Info** menu item and verify the minor's demographic information (Figure 10-12).

Figure 10-12: PHR Patient Web Portal - My Info: About Me section

> **Note:** If the demographic information does not match the minor's information, delete access to this PHR account (Section 10.3) and repeat the steps for granting access to the minor's PHR (Section 10.1).

10.2　Update Access to a Minor's PHR

A parent, legal guardian, court appointed guardian, or individuals acting *in loco parentis* that have access to a minor's PHR sections may change the access type.

> **Note:** The individual does not have to be an IHS patient to be given access to the minor's PHR. However, the individual listed on the approved IHS-810 form must have a registered PHR account at a minimum.

10.2.1　Update Access Type

To update the type of PHR access for the individuals listed on the approved IHS-810 form, do the following:

1. Go to the PHR Patient Web Portal website at https://phr.ihs.gov.

2. Logon to the PHR Patient Web Portal as in Section Figure 6-1, Step 1. The My Health Records page opens (Figure 10-13).

3. Click the **Manage My Accounts** link on the **My Health Records** page (Figure 10-13). The **My Accounts** page opens (Figure 10-14).
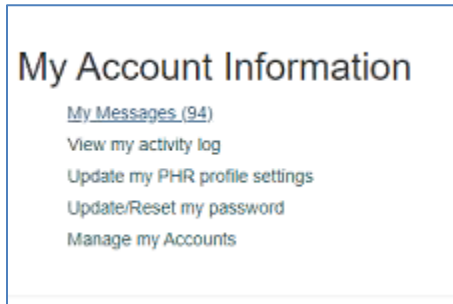
Figure 10-13: PHR Patient Web Portal - My Health Records

4. Click the **Add/Update Account Access** link on the **My Accounts** page (Figure 10-14). The **Manage Access to my Personal Health Record** page opens (Figure 10-15).
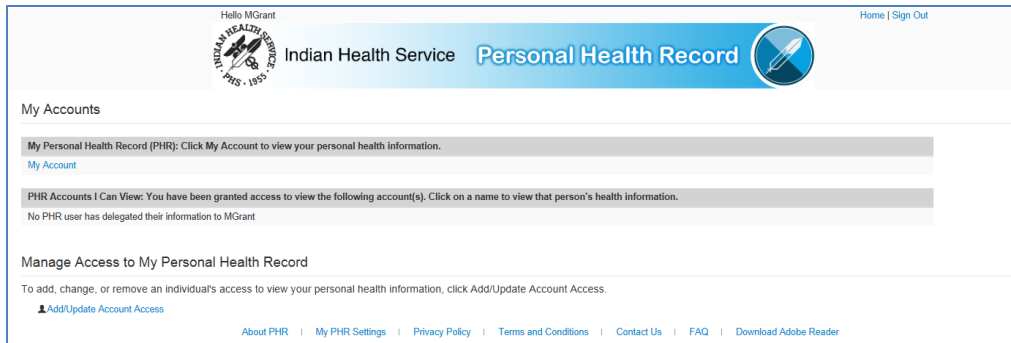
Figure 10-14: PHR Patient Web Portal - My Accounts

5. Click the pen and paper icon under the **Update Access** column on the **Manage Access to my Personal Health Record (PHR)** page for the user you want to update (Figure 10-15). The **Update Access** page opens (Figure 10-16)

Figure 10-15: PHR Patient Web Portal - Manage Access to my Personal Health Record page with User Access Displayed: Full Access

6. Click the **Edit Access Type** link in the **Access Information** pane on the **Update Access** page (Figure 10-16). The **Edit Access Types** page opens (Figure 10-17).

Figure 10-16: PHR Patient Web Portal - Update Access for delegated user

a. To go back to the **Manage Access to my Personal Health Record (PHR)** page, click **Back**.

> **Note:** If the selected user's current type of access is Limited Access, the Hidden Sections pane will display. To edit hidden sections, see Section 10.2.2.

7. On the **Edit Access Type** page (Figure 10-17), choose an access type (see Section 10.1, Step 7) to grant to the user. Click **Update** to continue. You are returned to the **Update Access** page (Figure 10-16).

a. Click **Cancel** to return to the Update Access page.

> **Note:** If the approved IHS-810 form has limitations regarding the data that can be viewed in the minor's PHR, do not select the Full Access type.

Figure 10-17: PHR Patient Web Portal - Edit Access Types

8. Verify that the type of access was updated on the **Update Access** page (Figure 10-18).

> **Note:** If the type of access was updated to Limited Access, the Hidden Sections pane will display. To edit blocked sections, see Section 10.2.2.

Figure 10-18: PHR Patient Web Portal - Update Access for delegated user page with the Hidden Sections Pane Added

   a. Click **Back** to go back to the **Manage Access to my Personal Health Record (PHR)** page.

9. Log off of the minor's PHR and verify the user given access can view the minor's health information based on the updated access type (Full or Limited).

a. Have the individual logon to the PHR using their PHR account.

b. On the **My Accounts** page (Figure 10-19), click the minor's PHR account under the **PHR Accounts I Can View** section.
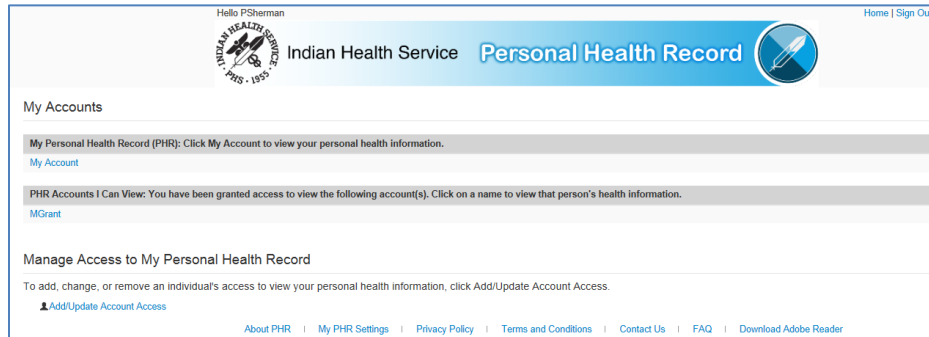
Figure 10-19: PHR Patient Web Portal - My Accounts

c. Select one of their facilities (preferably your facility) from the **My Health Records** page. The My Health Records Page Facility List opens (Figure 10-20).
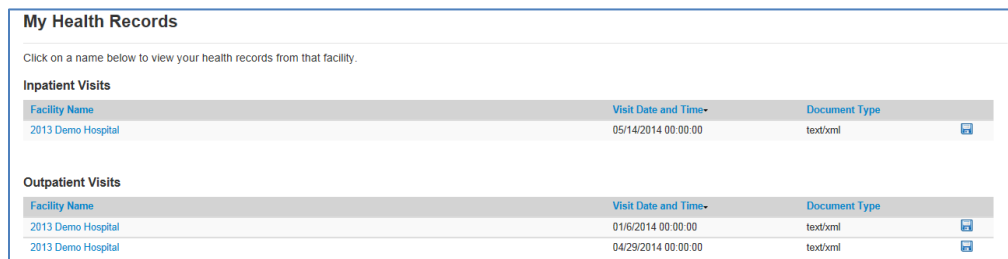
Figure 10-20: PHR Patient Web Portal - My Health Records Page Facility List

d. Verify the individual can view the minor's health information (Figure 10-21) based on the updated access type (Full or Limited).
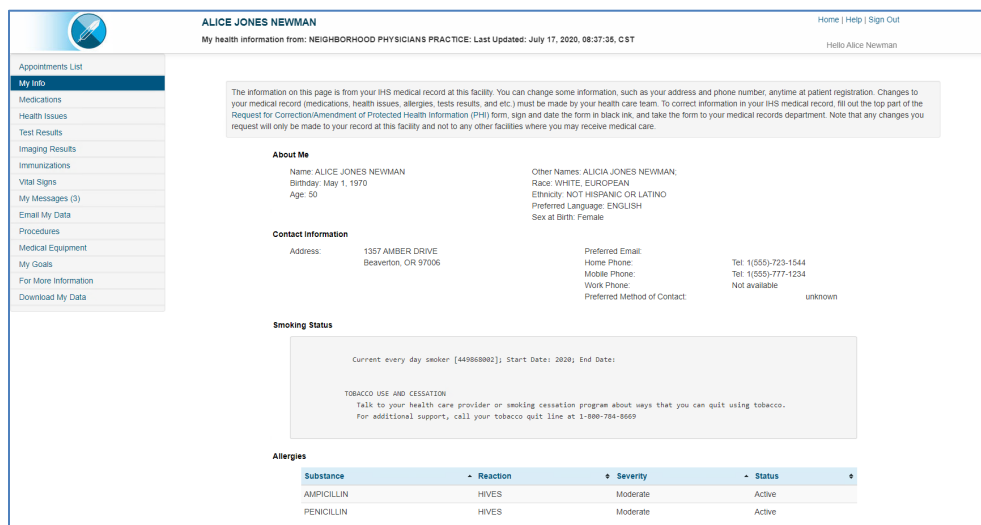
Figure 10-21: PHR Patient Web Portal - Full Access: Displays All Menus selected for access

> **Note:** If the individual can view more or less information than is expected based on the access type, verify the type of access granted to the individual by repeating Steps 1 through 8 . If the individual's access type is Limited, edit the individual's blocked sections (Section 10.2.2).

10.2.2   Edit Hidden Sections

To edit the blocked sections to the individuals listed on the approved IHS-810 form with the Limited Access type, do the following:

1. Complete Steps 1 through 4 in Section 0.

2. Click the pen and paper icon under the **Update Access** column on the **Manage Access to my Personal Health Record (PHR)** page for the user you want to update access (Figure 10-22). The Update Access for delegated user page with the Hidden Sections pane opens (Figure 10-23).

Figure 10-22: PHR Patient Web Portal - Manage Access to my Personal Health Record page with User Access Displayed: Limited Access

3. Click the **Edit Hidden Sections** link in the **Hidden Sections** pane on the **Update Access** for delegate user page (Figure 10-23). The Edit Personal Health Record (PHR) Section Access page opens (Figure 10-24).

Figure 10-23: PHR Patient Web Portal - Update Access for delegated user page with the Hidden Sections pane

    a.   Click **Back** to go back to the **Manage Access to my Personal Health Record (PHR)** page.

4. On the **Edit Personal Health Record (PHR) Section Access** page (Figure 10-24), follow the instructions on the screen to select or de-select the PHR sections to grant the user access and click **Update** to continue. The Update Access page opens (Figure 10-25).

> **Note:** By default, the **Download My Data Section** is unchecked, which prevents the user from downloading the patient's visit information.

    a.   Click **Cancel** to cancel and return to the **Manage Access to my Personal Health Record (PHR)** page.

Figure 10-24: PHR Patient Web Portal - Edit Personal Health Record (PHR) Section Access

5. Verify the **Hidden Sections** pane was updated on the **Update Access** for delegate user page (Figure 10-25).
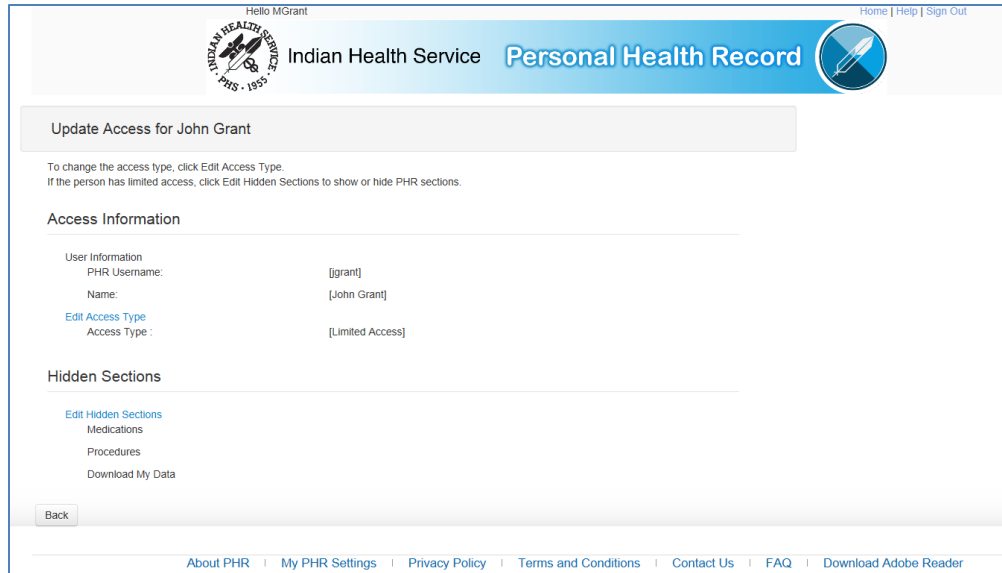
Figure 10-25: PHR Patient Web Portal - Update Access for delegated user page with the Hidden Sections pane

    a.   Click **Back** to go back to the **Manage Access to my Personal Health Record (PHR)** page.

6.   Log off of the minor's PHR and verify the user given access to the minor's PHR can view the minor's health information for the sections granted access.

    a.   Have the individual logon to the PHR using their PHR account.

    b.   On the **My Accounts** page, click the minor's PHR account under the **PHR Accounts I Can View** section (Figure 10-26). The My Health Records Page Facility List opens (Figure 10-27 ()).
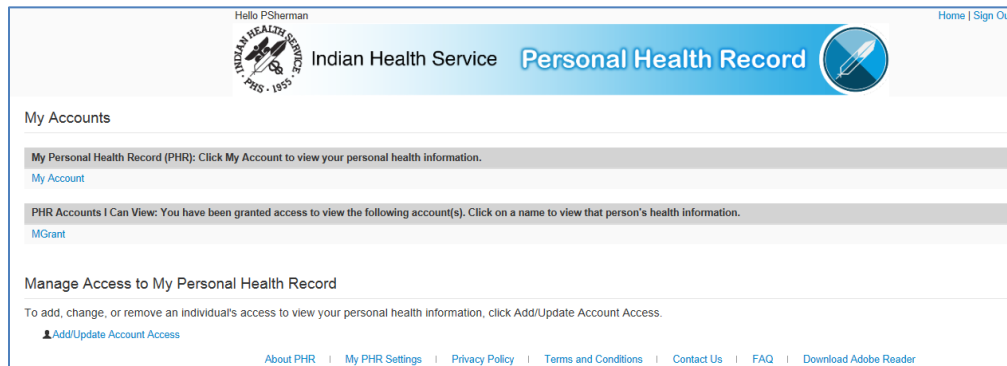
Figure 10-26: PHR Patient Web Portal - My Accounts

    c.   Select one of their facilities (preferably your facility) from the **My Health Records** page (Figure 10-27). The Limited Access: Displays Available Menus opens (Figure 10-28).

Figure 10-27: PHR Patient Web Portal - My Health Records Page Facility List

  d. Verify the individual can view the minor's health information based on the updated access type (Full or Limited; Figure 10-28).

Figure 10-28: PHR Patient Web Portal - Limited Access: Displays Available Menus

> **Note:** If the individual can view more or less information than is expected based on the access type, verify the type of access granted to the individual by repeating Steps 1 through 5.

10.3 Delete Access to a Minor's PHR

In some cases, access to a minor's PHR by a parent, legal guardian, court appointed guardian, or individuals acting *in loco parentis* will need to be removed. These cases include but are not limited to; abuse of PHR privileges, the primary provider requests access removal, court order, or the minor becomes emancipated, etc.

To delete access to the individuals listed on the approved IHS-810 form, do the following:

1. Go to the **PHR Patient Web Portal** website at https://phr.ihs.gov (Figure 10-29).

2. Logon to the PHR Patient Web Portal by entering the minor's PHR **Username** and **Password** and click **Login**. The My Health Records page opens (Figure 10-30).

Web Portal Administrator Manual   Grant Access to a Minor's PHR
September 2020

106

Figure 10-29: PHR Patient Web Portal Logon

3. Click the **Manage My Accounts** link on the **My Health Records (Home)** page (Figure 10-30). The My Accounts page opens (Figure 10-31).
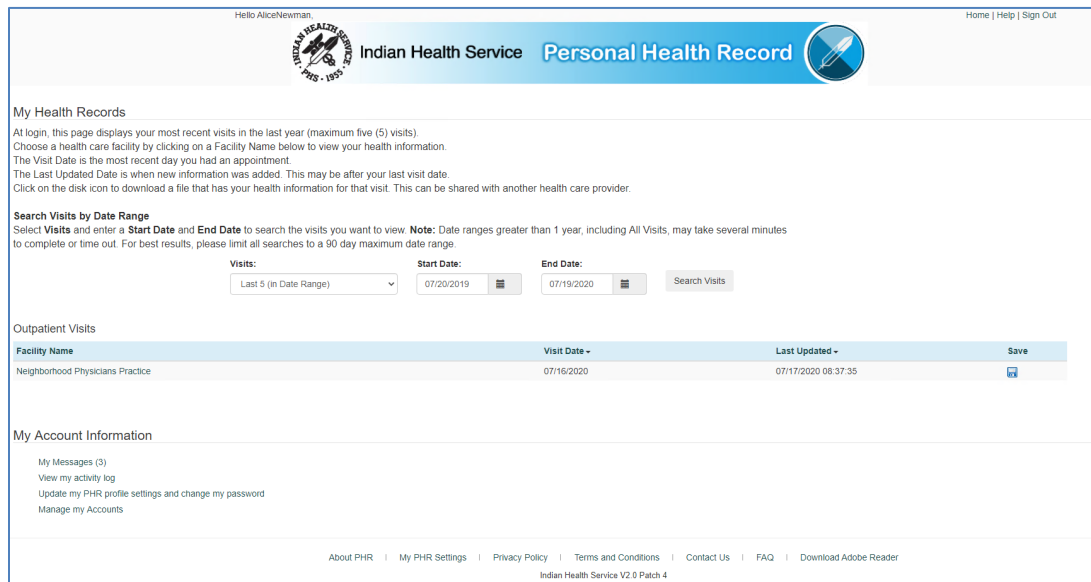
Figure 10-30: PHR Patient Web Portal - My Health Records

4. Click the **Add/Update Account Access** link at the bottom of the **My Accounts** page (Figure 10-31). The Manage Access to my Personal Health Record (PHR) page opens (Figure 10-32).
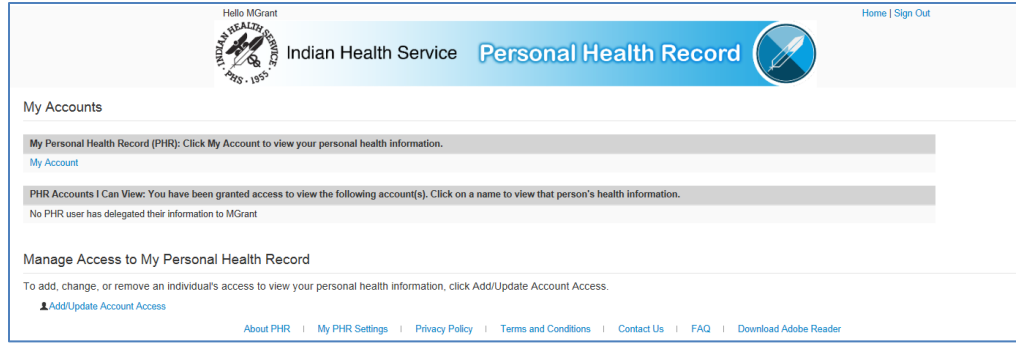
Figure 10-31: PHR Patient Web Portal - My Accounts

5. Click the red circle with a white x icon under the **Delete Access** column on the
    Manage Access to my Personal Health Record (PHR) page of the user for
    whom you want to remove access (Figure 10-32). The Are You Sure You Want
    To Revoke Access page opens (Figure 10-33).

Figure 10-32: PHR Patient Web Portal - Manage Access to my Personal Health Record page
            with User Access Displayed

6. On the **Are you sure you want to revoke access for this user** dialog, click **OK**
    to delete the user's access.

    a. To go back to the **Manage Access to my Personal Health Record (PHR)**
        page without deleting the user's access, click **Cancel**.
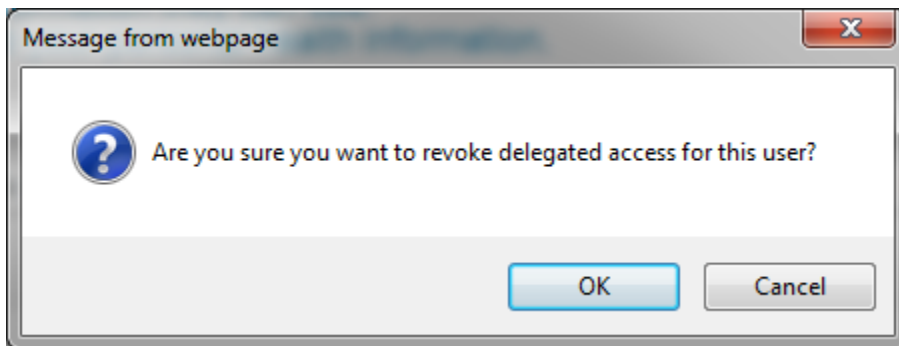
Figure 10-33: Are you sure you want to revoke access for this user dialog

7. Verify the user's access was removed on the **Manage Access to my Personal Health Record (PHR)** page (Figure 10-34).

> **Note:** If the individual's whose access to the minor's PHR is being revoked is with the PHR Administrator revoking access, ask the person to logon to the PHR and verify they cannot view the minor's account.

Figure 10-34: PHR Patient Web Portal - Manage Access to my Personal Health Record page with No User Access Displayed

10.4   Emancipated Minors

Minors who have been emancipated according to applicable law can be granted access to the PHR. Before an emancipated minor can access the PHR and view their IHS Medical Record, the emancipated minor will need to complete the following steps:

1. Register to use the PHR (see Section 6.1).

2. The patient goes to their IHS facility to complete the in-person identity verification process (See Section 6.2).

   a. Provide proof that he or she has been emancipated according to applicable law. If it is unclear which law applies to an emancipated minor, consult the Area HIM Consultant or the Office of General Counsel (OGC).

   b. Provide a copy of a court's decision that he or she is an emancipated minor as of today or were in legal guardianship immediately before reaching the age of being an adult in your state. The court must be located in the state of legal residence in which the PHR account is being processed as emancipated.

   c. The PHR Registrar verifies the patient's identity

3. The PHR Registrar processes the patient's application and links the patient's registered PHR account with their IHS Medical Record (see Section 6.3).

4. The emancipated minor logs on to the PHR at https://phr.ihs.gov (see Section 6.4)

> **Note:** Although an emancipated minor is under the age of 18, emancipated minors are considered to be of legal age and their own legal guardian. Therefore, the PHR will not filter sensitive information (e.g., family planning, drug/alcohol treatment, domestic violence, and STIs) for these users.

10.4.1   Grant Non-PHR Linked Emancipated Minors Access to the PHR

To grant an emancipated minor who does not have a linked PHR account access to the PHR, do the following:

1. Complete Steps 1 through 2 described in Section 10.4. The Detailed Patient Profile page for un-emancipated minor opens (Figure 10-35).

2. Complete Steps 1 through 7 in Section 7.1 and click **Emancipated Minor**. The **Manage Patient Profile (Update Emancipated Minor)** dialog opens (Figure 10-36).

Figure 10-35: Manage Patients - Detailed Patient Profile page for un-emancipated minor

3. Click **OK** on the **Manage Patient Profile (Update Emancipated Minor)** dialog (Figure 10-36).
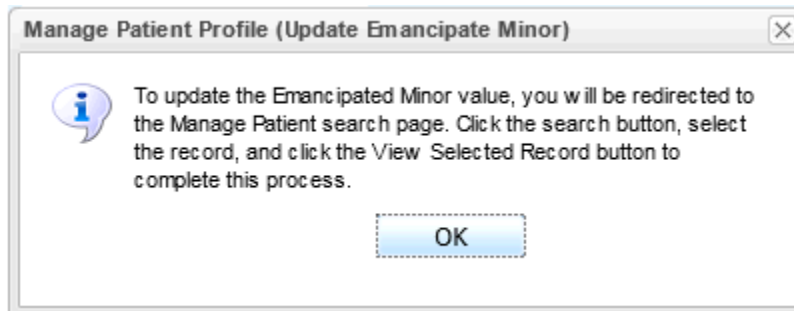
Figure 10-36: Manage Patient Profile (Update Emancipated Minor)

> **Note:** A database update is required to update the emancipated minor status. As a result, clicking the **OK** button will redirect to the Admin user to the Manage Patients page (Figure 7-2), which will invoke the call to update the database.

4. On the **Manage Patients** search page (Figure 7-2), leave the search settings as is and click **Search**. The **Manage Patients - Search** results page opens (Figure 7-4).

5. Select the PHR user account from the returned search results (Figure 7-4) and then click **View Selected Record**. The **Manage Patients - Detailed Patient Profile** page for emancipated minor opens (Figure 10-37).

6. The Emancipated Minor status will be updated to **Yes** and the **Emancipated Minor** button will be updated to **Not Emancipated Minor** (Figure 10-37).
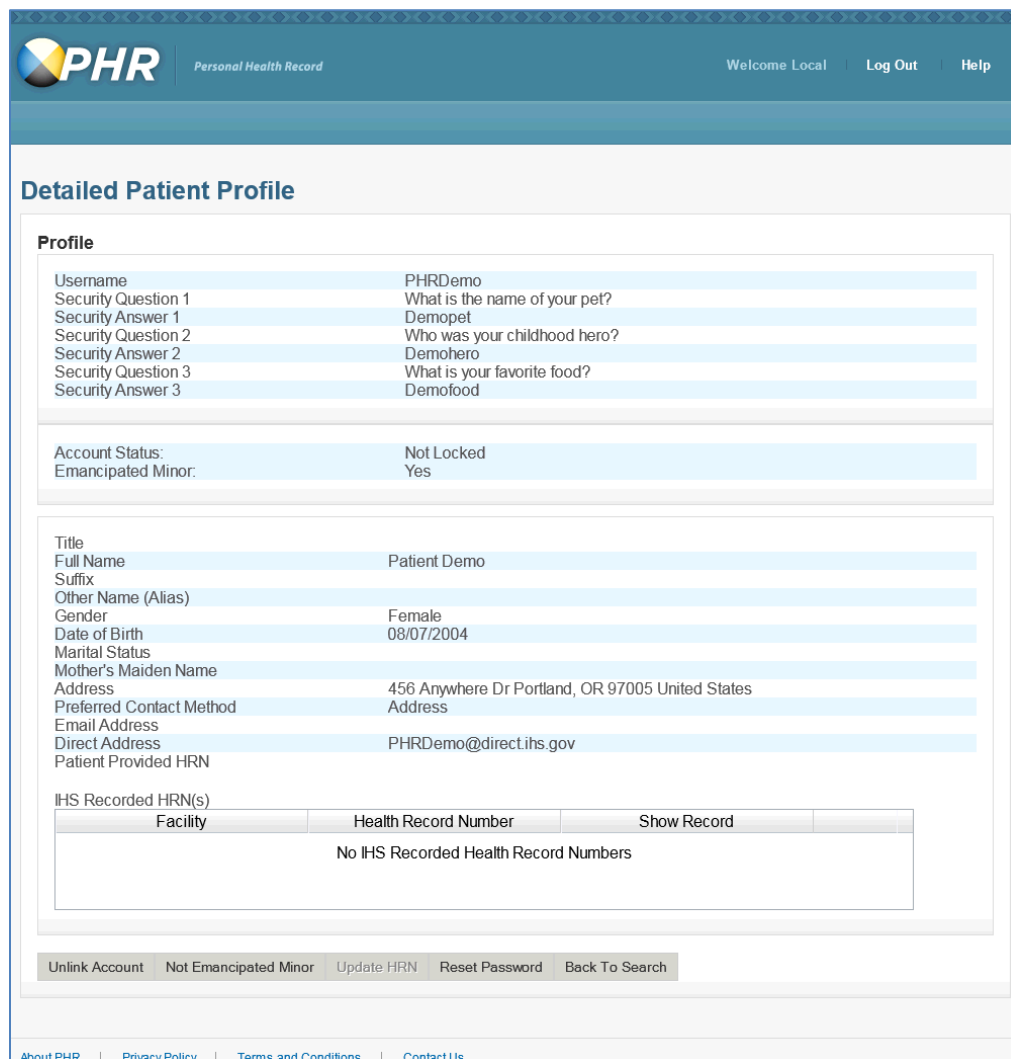
Figure 10-37: Manage Patients - Detailed Patient Profile page for emancipated minor

7. Complete Steps 3 and 4 in Section 10.4 to verify PHR access.

> **Note:** Once the emancipated minor turns 18, the account will automatically be updated by removing emancipated minor functionality. These accounts will remain active and linked.

10.4.2 Update a Minor's Linked PHR Account as an Emancipated Minor

Minors who have a PHR account and have been granted access to the PHR as defined in Sections 10.0 and 10.1 can be updated as an emancipated minor.

To update a minor's linked PHR account to an emancipated minor, do the following:

1. Complete Step 2 in Section 10.4.

2. Remove any access to the minor's PHR account as defined in the approved IHS-810 form described in Section 10.0.

3. Complete the steps in Section 10.3 for each user with access to the minor's PHR account.

> **Note:** If the My Accounts page is displayed skip Step 4.

4. Complete Steps 1 through 7 in Section 7.1 and click **Emancipated Minor** (Figure 10-35). The **Manage Patient Profile (Update Emancipated Minor)** dialog opens (Figure 10-38).

5. Click **OK** on the **Manage Patient Profile (Update Emancipated Minor)** dialog (Figure 10-38).
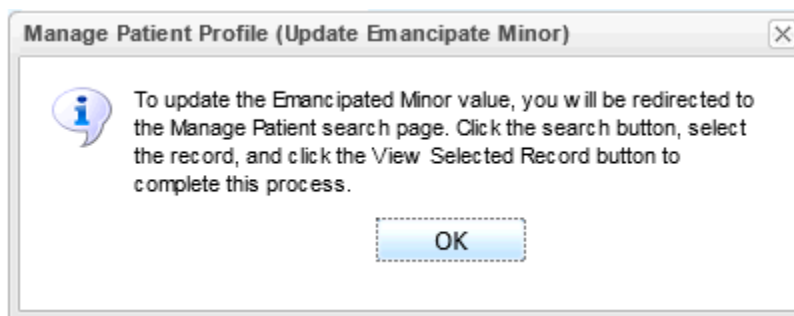
Figure 10-38: Manage Patient Profile (Update Emancipated Minor)

> **Note:** A database update is required to update the emancipated minor status. As a result, clicking the **OK** button will redirect to the Admin user to the Manage Patients page (Figure 7-2), which will update the database.

6. On the **Manage Patients** search page, leave the search settings as-is and click **Search** (Figure 7-2). The Manage Patients - Search results page opens (Figure 7-4).

7. Select the PHR user account from the returned search results and then click **View Selected Record** (Figure 7-4). The Manage Patients - Detailed Patient Profile page for emancipated minor opens (Figure 10-36).

8. The Emancipated Minor status will be updated to **Yes** and the **Emancipated Minor** button will be updated to **Not Emancipated Minor** (Figure 10-36).

> **Note:** To ensure all delegation was removed, the account will automatically be unlinked as part of the PHR emancipation process and must be relinked before the emancipated minor can view their IHS Medical Record in the PHR.

9. Complete Steps 3 and 4 in Section 10.4 to verify PHR access.

> **Note:** Once the emancipated minor turns 18, the account will automatically be updated by removing emancipated minor functionality. These accounts will remain active and linked.

10.4.3   Remove Emancipated Minor Status

In some cases, an emancipated minor's status may need to be revoked (set to No). These may include one of the following:

- The minor's account was updated as an emancipated minor by mistake.

- Although rare, a court may revoke a minor's emancipation status under extreme circumstances.

> **Note:** If a court has revoked a minor's emancipated status, documented proof (a copy of the court's decision) that the emancipated minor's status has been revoked is required to remove the Emancipated Minor status.

To remove and reset an emancipated minor's PHR account back to a standard PHR minor account, do the following:

1. Complete Steps 1 through 7 in Section 7.1 and click **Not Emancipated Minor**. The Manage Patients - Detailed Patient Profile page for emancipated minor opens (Figure 7-5).

2. Click **OK** on the **Manage Patient Profile (Update Emancipated Minor)** dialog (Figure 10-39).
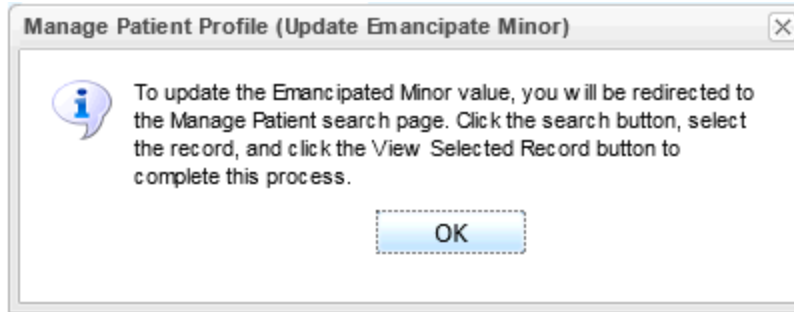
Figure 10-39: Manage Patient Profile (Update Emancipated Minor)

> **Note:** A database update is required to update the emancipated minor status. As a result, clicking the **OK** button will redirect to the Admin user to the Manage Patients page (Figure 7-2), which will invoke the call to update the database.

3. On the **Manage Patients** search page (Figure 7-2), leave the search settings as is and click **Search**.

4. Select the PHR user account from the returned search results (Figure 7-4), and then click **View Selected Record**.

5. The Emancipated Minor status will be updated to **No** and the **Not Emancipated Minor** button will be updated to **Emancipated Minor** (Figure 10-40).

> **Note:** To ensure all delegation was removed, the account will automatically be unlinked as part of the PHR un-emancipation process and must be relinked before granting access to the un-emancipated minor's PHR.
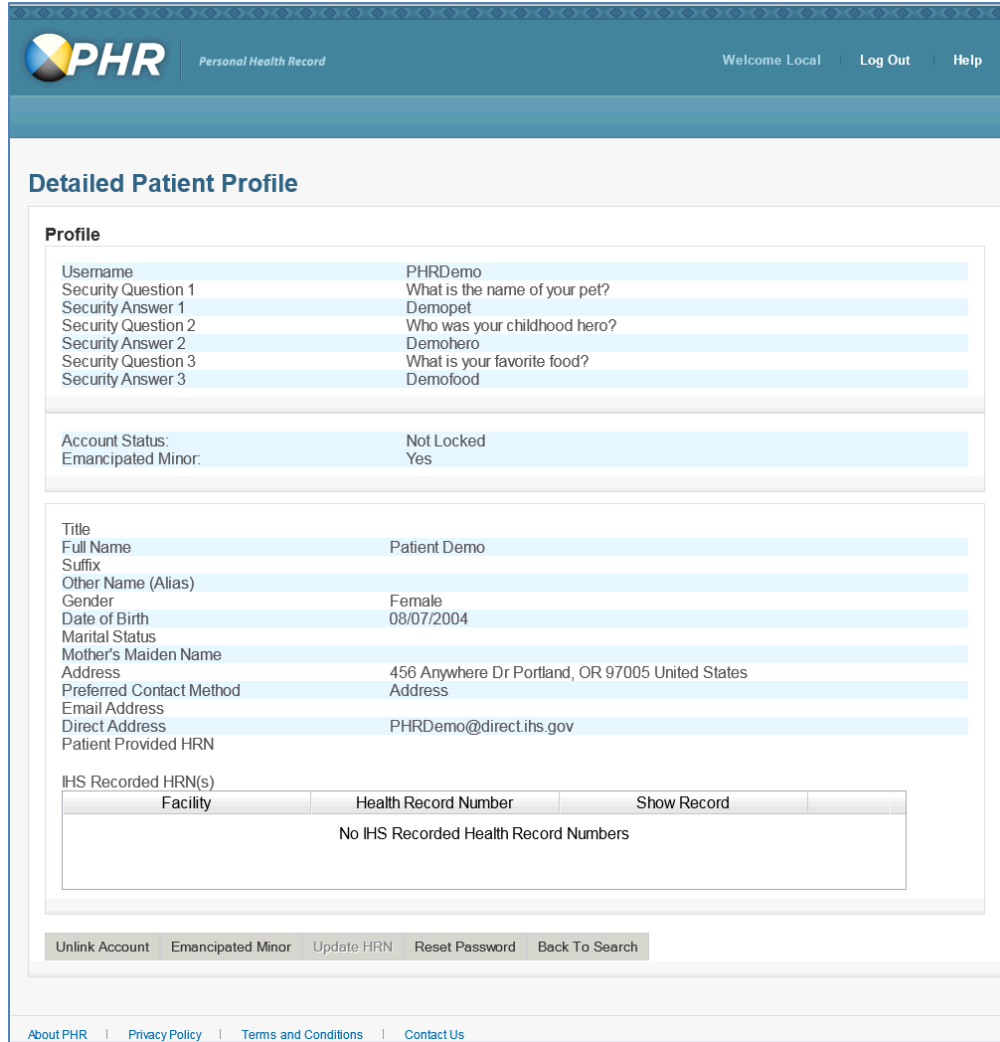
Figure 10-40: Manage Patients - Detailed Patient Profile page for un-emancipated minor

6. Complete the steps in Sections 10.0 and 10.1 to reestablish access to a minor's PHR, as needed.

11.0   Report a Breach or Misuse of the PHR

All PHR administrators must report inappropriate or suspicious activities, such as misuse of the PHR system (PHR Administrator Web Portal or PHR Patient Web Portal applications) and PHI/PII under the PHR system, using the IHS Incident Response Team (IRT) process and/or local facility procedures.

Additionally, local administrators shall advise the Area and/or local Privacy Officer of the incidents and include them in the investigation, response, and any subsequent notification that is required by law. For reporting, facilities on the IHS D1/Active Directory are required to use IRT procedures at https://www.ihs.gov/IHM/pc/part-8/p8c9/.

All Tribal and Urban facilities are required to follow their local policies and procedures and required to notify IHS of such breach using IRT Incident Response Form (https://www.ihs.gov/IHM/pc/part-8/p8c9/).

12.0   Technical Support

IHS RPMS DIRECT Information Technology (IT) support is based on the principle of tiered levels of support (Figure 12-1).

The levels of support provided at each tier are as defined by the OIT Standards & Policies (See https://www.ihs.gov/oit/operations/). See local policies and procedures for further information.

Figure 12-1: Flow of Tiered Service Support (OIT Customer Service handbook Figure 1)

12.1   Tier 1

PHR Tier 1 support is provided by the local Service Unit/Facility. Tier 1 is the basic level of customer support related to IT hardware, software, and telecommunications. Examples would include access request, reset of passwords, training, PHR Patient Web Portal issues, and other PHR related questions.

12.2   Tier 2

PHR Tier 2 support is provided by the Area IT office and Area Administrators. Tier 2 supports provide an intermediate level of customer support related to PHR administrative access, or system related issues. Examples would include assistance in adding or terminating SU/FA, resetting of SU/FA Administrator passwords, or other PHR related questions.

12.3   Tier 3

PHR Tier 3 support is provided by IHS OIT. Examples would include troubleshooting errors in the PHR system or maintenance of the PHR system.

12.4   Requesting Help

PHR administrators should follow the Tier 1, Tier 2 and Tier 3 process for support. As noted on the IHS website at https://www.ihs.gov/oit/operations/, Tier 3 support from field units will be directed to the associated AO for initial support.

12.5   E-Mail

The IHS IT Service Desk can be reached by sending e-mail message to
itsupport@ihs.gov.

12.6   Phone

The IHS IT Service Desk can be reached via phone at the number listed below. See
the OIT Customer Service Handbook for more information.

- 1-888-830-7280 (Toll Free)

13.0   Appendices

Appendix A contains additional information about PHR Recorded Event Types.
Appendix B contains information about security and role-specific responsibilities.

Appendix A   PHR Recorded Event Types

The PHR records the following event types for each specific role. This Section lists the PHR recorded event types, a brief description of each event, and the role the event type is recorded.

Table A-1: Recorded Event Types

Event Display Name	Event Description	Severity	Nat Admin	AO Admin	SU/FA	Registrar	Patient
Event Logging Failure	Fails to purge event log and other non-specified system events	High	x				
HIE Service Connection Failure	Problems with the IHS HIE service	High	x				
MPI Service Connection Failure	Problems with the IHS MPI service	High	x				
User Not Found in PHR DB	Administrator or Patient PHR account not in the PHR SQL database	High	x				
Event Logging Successful	Successfully purged event log and other non-specified system events	Low	x				
Admin Account Create Failure	Fails to create an Administrator account or exceeds the permitted number of administrative accounts.	High	x	x	x		
Create Temporary Password Failure	Fails to create a temporary password for an administrator or PHR User account	High	x	x	x	x	
Audit Report Export	Exports audit report		x	x	x	x	
Audit Report Generation	Generate an audit report		x	x	x	x	
Update Emancipation	Updates emancipation information		x	x	x	x	
Update Preferred Facilities	Updates preferred facilities		x	x	x	x	

Event Display Name	Event Description	Severity	Nat Admin	AO Admin	SU/FA	Registrar	Patient
Login Failure	Administrator or Patient fails to successfully logon to the PHR Application	High	x	x	x	x	x
Patient Facility Update Failure	Fails to complete the HRN update functionality.	High	x	x	x	x	
Unlink Patient Record Failure	Fails to unlink a registered PHR User with his or her IHS Medical Record	High	x	x	x	x	
Admin Account Inactivate Successful	Successfully inactivates an Administrator account	Low	x	x	x		
Admin Account Reactivate Successful	Successfully reactivates an Administrator account	Low	x	x	x		
Admin Update Successful	Successfully updates an Administrator account	Low	x	x	x	x	
Login Successful	Administrator or Patient successfully logs into the PHR Application	Low	x	x	x	x	x
Logout	Administrator or Patient logs out of the PHR Application	Low	x	x	x	x	x
Admin Account Create Successful	Successful creation of an Administrator account	Medium	x	x	x		
Admin Account Inactivate Failure	Fails to inactivate an Administrator account	Medium	x	x	x		
Admin Account Reactivate Failure	Fails to reactivate an Administrator account	Medium	x	x	x		
Admin Update Failure	Fails to update an Administrator account	Medium	x	x	x	x	
Create Temporary Password Successful	Successfully creates a temporary password for an Administrator or PHR User account	Medium	x	x	x	x	

Event Display Name	Event Description	Severity	Nat Admin	AO Admin	SU/FA	Registrar	Patient
Unlink Patient Record Successful	Successfully unlinks a registered PHR user with his or her IHS Medical Record	Medium	x	x	x	x	
Blue Button Download Failure	Blue button fails to download health information	High					x
Facility Not Found in PHR DB	PHR is unable to locate the patient facility in the PHR database	High				x	
Incorrect Security Question Answers	User answers one or more security questions incorrectly when attempting to reset their password.	High					x
No Visit Documents Found	Unable to locate documents for the patient in the central IHS HIE	High					x
Process Patient Application Failure	Fails to process a registered patient PHR application	High				x	
User Forgets UserName	PHR user clicks on the forgot username link and retrieves their PHR username	High					x
User Registered Failure	PHR user fails to register successfully to use PHR from the Patient Application	High					x
Blue Button Download Successful	Patient downloads health information	Low					x
Medication Refill Request	User request a medication refill request using the Request Refill button.	Low					x
User Accepts Privacy Policy	Patient accepts the privacy policy during the PHR registration process from the Patient Application	Low					x

Event Display Name	Event Description	Severity	Nat Admin	AO Admin	SU/FA	Registrar	Patient
User Accepts Terms And Conditions	Patient accepts the terms and conditions for PHR use during the PHR registration process from the Patient Application	Low					x
User Adds Delegation	PHR user adds delegated user to view their PHR	Low					x
User Registered Successful	Patient successfully registers to use PHR from the Patient Application	Low					x
User Select More Info Button	User selects the info button from any page that includes the More Info button/link to Medline plus	Low					x
User Update Delegation	User updates delegated user access to view their PHR	Low					x
View Blue Button Section	User views the Download My Data Page	Low					x
View Health Issues Section	User views the Health Issues page	Low					x
View Hospital Admissions Section	User views the Hospital Admissions page	Low					x
View Immunizations Section	User views the Immunizations page	Low					x
View Medications Section	User views the Medications page	Low					x
View More Information Section	User views the For More Information page	Low					x
View My Info Section	User views on the My Info page	Low					x
View My Goals Section	User views on My Goals page	Low					x
View Imaging Results Section	User views on the Imaging Results page	Low					x

Event Display Name	Event Description	Severity	Nat Admin	AO Admin	SU/FA	Registrar	Patient
View Medical Equipment Section	User views on the Medical Equipment page	Low					x
View Procedures Section	User views on the Procedures page	Low					x
View Secure Messages Section	User views on the My Messages page	Low					x
View Test Results Section	User views on the Test Results page	Low					x
View Visit CCDA Document	User selects one of their visit records	Low					x
View Email My Data Section	User views on Email My Data page	Low					x
View Vital Signs Section	User views on the Vital Signs page	Low					x
Process Patient Application Successful	Successfully processes a registered patient PHR application	Medium				x	
User Delete Delegation	PHR user deletes delegated user to view their PHR	Medium					x
User Downloads CCDA Document	PHR user downloads their raw data (clicks the save button on the landing page)	Medium					x
User Rejects Privacy Policy	Patient rejects the privacy policy during the PHR registration process from the Patient Application	Medium					x
User Rejects Terms And Conditions	Patient rejects the terms and conditions for PHR use during the PHR registration process from the Patient Application	Medium					x
User Update Security Questions	User updates their security questions/answers	Medium					x

Event Display Name	Event Description	Severity	Nat Admin	AO Admin	SU/FA	Registrar	Patient
User Updates Password	User updates/changes their password.	Medium					x
User Updates Profile Successful	User updates their personal details	Medium					x

Appendix B   Rules of Behavior

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

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

- For a listing of general ROB for all users, see the most recent edition of *IHS General User Security Handbook* (SOP 06-11a).

- For a listing of system administrators/managers rules, see the most recent edition of the *IHS Technical and Managerial Handbook* (SOP 06-11b).

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

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

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

B.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).

B.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.

B.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.

B.1.3   Accountability

RPMS users shall

- Behave in an ethical, technically proficient, informed, and trustworthy manner.

- Log off 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.

B.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.

B.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.

B.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 logon attempts within a specified time period (e.g., one hour).

B.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 logon 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.

B.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.

B.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.

B.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 a period of inactivity.

B.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.

B.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.

B.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 the following 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

B.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.

B.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
AO	Area Office
HIE	Health Information Exchange
HIM	Health Information Management
IHS	Indian Health Service
ISSO	Information System Security Officer
ITAC	Information Technology Access Control
MPI	Master Patient Index
OIT	Office of Information Technology
PHI	Protected Health Information
PHR	Personal Health Record
PII	Personally Identifiable Information
RPMS	Resource and Patient Management System
SU/FA	Service Unit/Facility

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