IBM Phytel User Management

© Copyright IBM Corporation. 2019.

IBM Confidential

Before using this information and the product it supports, read the information in "Notices" at the end of this document.

Licensed Materials – Property of IBM

© Copyright IBM Corp. 2010, 2019.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM, the IBM logo, IBM Phytel, IBM Phytel Coordinate, IBM Phytel Transition, IBM Phytel Outreach, IBM Phytel Remind, IBM Phytel Engage, the Phytel logo, and combinations thereof are trademarks of IBM Corporation, registered in many jurisdictions worldwide.

Contents

© Copyright IBM Corporation. 2019.

IBM Confidential

Accessing User Administration

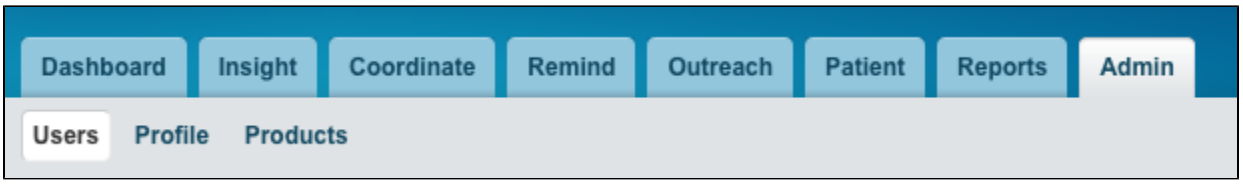
Individuals within each organization, typically Practice Managers, are set up as application administrators. Application administrators can perform the following tasks:

- Create new users
- Search for an existing user to make modifications
- Unlock users who have been locked out of the system
- Manage a user's group assignment

Permissions Needed

If you do not have the appropriate permissions to access this tab, you should contact your administrator or project manager.

To access the administrative feature, after logging in, select the **Admin** tab.



This page allows the administrator to search for existing users as well as create new users and manage existing users.

© Copyright IBM Corporation. 2019.

IBM Confidential

Searching for a User

When viewing the **Users** page, the list of all **Active**, **Inactive**, and **Locked** users is displayed and sorted in ascending order by **Name**.

> **Deleted Users**
>
> If a user has been deleted, then they are no longer accessible through the user interface and must be setup again; you may not activate a previously deleted user.

You can use the filters above the user list to quickly locate specific users.

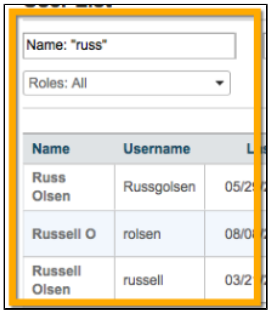
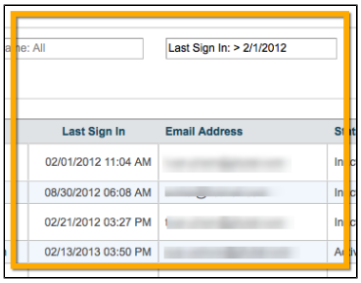
- **Name**, **Username**, **Email Address**: Type text directly into any of these fields, and press **Enter** or **Tab**. The list automatically refreshes, displaying only those records that contain the text you input for the applicable field. If you want to see users who do not have an email address, enter a **-** in the **Email Address** date field, and press **Enter** or **Tab**.
- **Last Sign In**: Type a date, and press **Enter** or **Tab**; the list automatically refreshes, displaying only those users that have a **Last Sign In** value greater than the date you specify. If you want to see users who have not logged in, enter a **-** in the **Last Sign In** date field, and press **Enter** or **Tab** .
- **Statuses**, **Roles**: You can select one or more of the values in their respective drop-down lists. Once selected, click anywhere outside of the drop-down list. It refreshes automatically, displaying only those users that have those selected values.

> **Status of a Locked user**
>
> A user's **System Locked** checkbox is clicked when they have too many consecutive unsuccessful logins; when their account is systematically locked, their **Status** remains the same. However, their **Status** displays as **Active (Locked)**. Users are only locked out for a defined time period (30 minutes), and they are unlocked to try again. An administrator can also edit a user's profile and manually unlock them.

You can enter criteria in one or more of the field filters. Each time, the list refreshes and narrows the results to only those users meeting all criteria input.

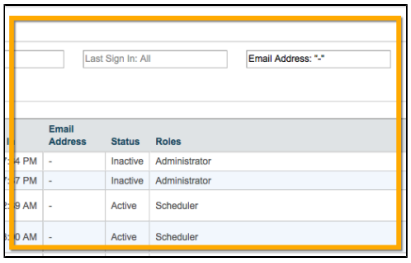
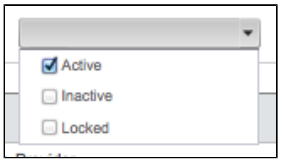
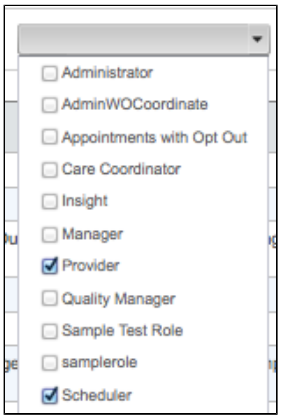
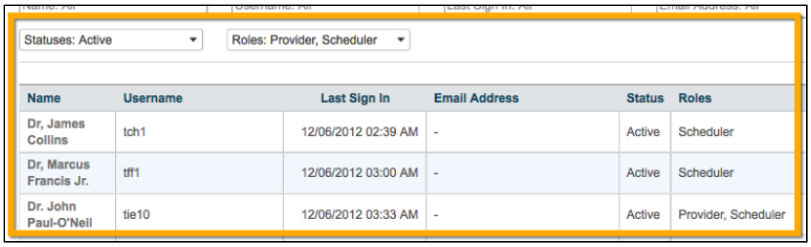
To clear a filter, navigate to it, and delete the text or date. For **Statuses** and **Roles**, if you deselect all values, then the list returns to the default of **All**.

Following are examples:

Filter	Input	Results
Name	russ	
Last Sign In	2/1/2012	

© Copyright IBM Corporation. 2019.

IBM Confidential

Email Address		
Statuses and Roles	Statuses filter:  Security Roles filter: 	

You can also sort by any of the columns by clicking on the appropriate column. When you locate the user, click on the user's name to show their details.

© Copyright IBM Corporation. 2019.

IBM Confidential

Creating a User

Only administrators have permissions to create a new user.

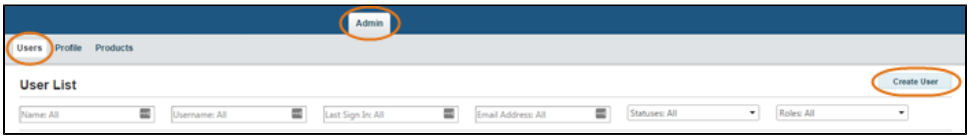
Before You Begin

To create a new user, you need the following information:

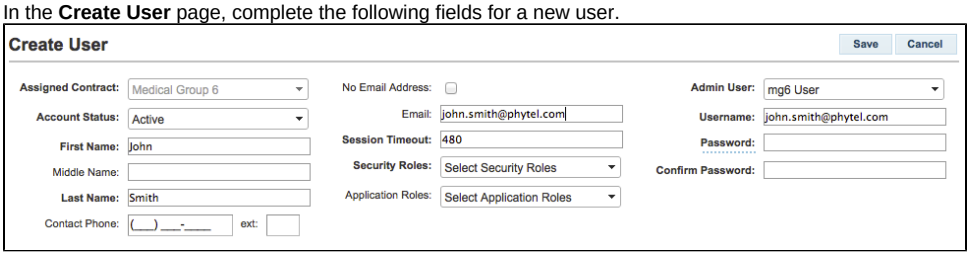
- User's contact information
- What functionality the user should be able to access
- What data the user should access. This includes:
  - Specific providers (Used for IBM® Phytel Outreach, IBM® Phytel Coordinate)
  - Specific schedules (Used for IBM® Phytel Remind)
  - Specific hospitals and units (Used for IBM® Phytel Transition)
- An understanding of the group structure, because this defines the providers and schedules a user can access

To create a user:

1. From the **Users** view in the **Admin** tab, click **Create User**.



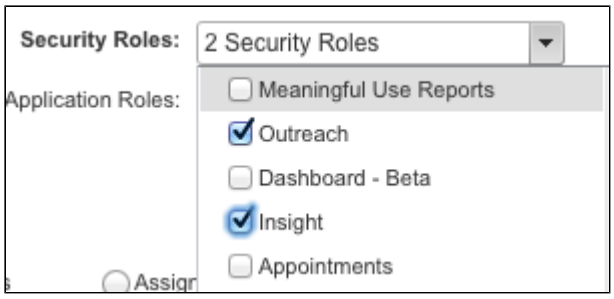
2. In the **Create User** page, complete the following fields for a new user.



Field	Required?	Comment
Assigned Contract	Yes	This field is automatically filled with the contract that the administrator logged in to create a user.
Account Status	Yes	Defaults to **Active**. A user can log on to an active account after it is created.
First Name	Yes	
Middle Name	No	
Last Name	Yes	
Contact Phone	No	
No Email Address	Yes	Defaults to unchecked. Only check if the user does not have an email address.
Email	No*	*This field is required if the **No Email Address** check box is not selected. The username defaults to the email address.
Session Timeout	Yes	Defaults to 480 minutes, or eight hours

© Copyright IBM Corporation. 2019.

IBM Confidential

Security Roles	Yes	Select one or more **Security Roles**. You can only assign roles that you have been assigned; available roles that you are not assigned appear disabled.  Choose the **Administrator** role when creating new users who must be able to create new users themselves. For more information about the available options, see Assigning Security Roles.
Application Roles	No	You do not have to select an **Application Role**. But you must designate a user as a **Care Manager** or **Provider** if you want the user to be listed as an option when using IBM Phytel Coordinate's **Care Manager** field.
Admin User	Yes	Defaults to the user creating the new user. If a user does not have an email address, then the Admin user receives emails if that user's password has been changed.
Username	Yes	Defaults to the email address, if entered. If users don't have email addresses, then we recommend using a naming convention. Example: first initial last name (ajefferson) User names are unique across the entire IBM® Phytel Atmosphere platform. If the user name is already in use, then it can help to add numbers to the end of the user name. Example: ajefferson2012 **Importance of Usernames** Information in the **Username** field is case-sensitive. User names must also be unique across the system. (Avoid using duplicate user names, even if they are not in your organization or have been archived.) Use your email address as your user name, as it is often the most unique. After you save the profile, you *cannot* change the username. Therefore, ensure it is correct before saving.
Password	Yes	Password must meet minimum requirements. Hover your mouse over the **Password** field to view the requirements.
Confirm Password	Yes	It must match the value entered in the **Password** field.
Group Assignment	Yes	Defaults to **Assign Specific Groups**. • Select the appropriate group or groups, and click the **>** action button to assign the group to the user. • To add all the groups, click the A**ssign All Groups** radio button. • To remove a group from a user, select the group in the **Groups Assigned** field, and click the **<** action button. After saving, you can view the schedules and providers associated with the assigned groups. For more information, see Assigning Groups.

3. Click **Save**.

© Copyright IBM Corporation. 2019.

IBM Confidential

Editing a User

A user can edit their own profile; however, they cannot modify any of the following fields:

- Group Assignments
- Security Roles
- Application Roles
- Account Status
- Username

A user can modify their security question and associated answer.

An administrator can modify all of the fields on a user's profile page except for the following:

- Assigned Contracts
- User Name
- Security Question and Answer

For security reasons, an administrator cannot view a user's security question and answer.

Password Resets

An administrator should avoid changing a user password. If a user does not recall their password, then they should click on the **Forgot Password** link on the **Sign In** page to reset it.

If an administrator resets a user's password, then an email is automatically sent to that user's email address, notifying them of the change. This is a precaution: If the user did not change their password or request that it be reset, then they must notify their administrator to avoid improper access.

© Copyright IBM Corporation. 2019.

IBM Confidential

Account Status

Each user is assigned one status, and all but **Inactive** users are managed by an administrator. When editing, you can change an account that is **Active**, **Inactive**, or **Locked** to any other status; however, you cannot access **Deleted** users in the user interface.

Status	User Access	Is Set by	Comment
Active	The user can access the application when valid credentials are entered.	Administrator	
Inactive	The user cannot access the application when valid credentials are entered.	System	The system automatically changes a user's status if the user has not logged in to the application for more than a year.
Locked	The user cannot access the application when valid credentials are entered.	Administrator	
Deleted	The user cannot access the application when valid credentials are entered.	Administrator	An administrator may not activate a deleted user.

© Copyright IBM Corporation. 2019.

IBM Confidential

System Locked

The **System Locked** check box is automatically enabled when a user has too many unsuccessful, consecutive logins within a 30-minute period. An administrator should avoid clicking this checkbox, and expect that the user will be locked out. The system will also automatically disable the checkbox after 30 minutes, allowing the user to attempt the login again. If you need to prevent a user from accessing the application, then set the user's **Account Status** to **Locked**.

© Copyright IBM Corporation. 2019.

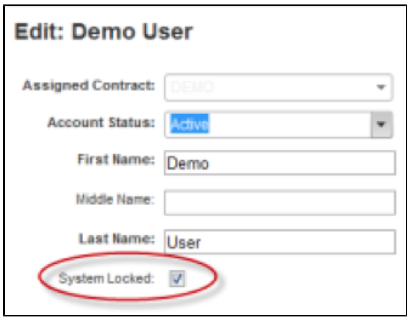
IBM Confidential

© Copyright IBM Corporation. 2019.

IBM Confidential

Common Actions

Besides managing basic user attributes, you can also do the following:

Action	How
Lock a user's account, so that they cannot access the application; often used when a user is terminated, is on temporary leave, or no longer has a need to access the application, but is still affiliated with the organization.	Change the user's **Account Status** to **Locked**
Unlock an account that has been locked due to too many consecutive, unsuccessful logins.	Disable the user's **System Locked** checkbox. 
Unlock an account that was manually locked; this could be due to the user changing positions or returning to work.	Change the user's **Account Status** to **Active**
Delete a user's account if the person is no longer a member of the organization, or the account was accidentally set up. **Deleted Users** Once a user is deleted, they cannot be reactivated. However, deleted user records are not permanently deleted; therefore, if you need to gather audit information, then IBM Phytel can assist. However, for security reasons, we recommend deleting users that are no longer affiliated with your organization to mitigate any risk of someone accessing the account without authorization.	Change the user's **Account Status** to **Deleted**

You may receive requests to change a user's password because they forgot it. For security purposes, we recommend that you instruct the user to click on the **Forgot Password** link on the **Sign In** page to reset their password.

© Copyright IBM Corporation. 2019.

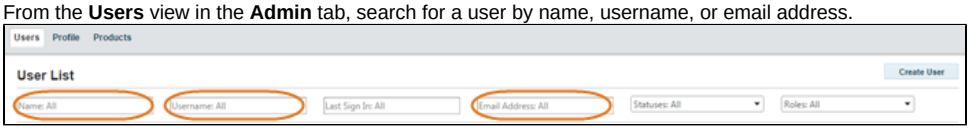
IBM Confidential

Security Roles

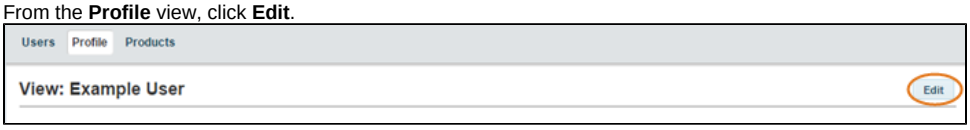
Security roles control users' access to features. For example, if a user needs to send notifications to patients when the facility is closed, then that user must have the Alert Notifications role.

> **Note**
>
> You must be assigned a role before you can assign it to other users.
>
> When new roles are available, you must request Client Care (PhytelClientCare@us.ibm.com) to assign you the new role.

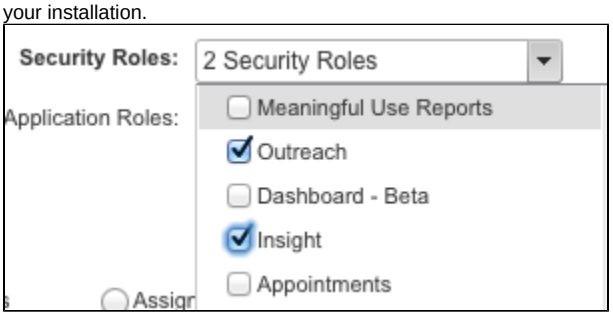
1. From the **Users** view in the **Admin** tab, search for a user by name, username, or email address.



2. In the search results table, click the name of a user to modify.
3. From the **Profile** view, click **Edit**.



4. From the **Security Roles** list, click the roles to assign to or remove from a user.
   See the Security Roles table below for a list of available roles. Some may not be applicable, as they depend on the products that are enabled for your installation.



5. Click **Save**.

Table: Security Roles

Security Role	Associated Product	Role Description
Appointments	IBM Phytel Remind	This role is for front office staff, schedulers, or practice managers, who schedule appointments for patients and handle different tasks related to patient check-in. The Appointments role allows schedulers and practice managers to view the patient responses to communication related to a scheduled appointment. Following are some actions these users can perform: • View patient responses to communications regarding their upcoming appointments on the **Confirmation Summary** page on the **Remind** tab • Search for patients using the **Patient Search** field • View the **Patient Summary** pop-up page, which lists historical patient communications and opt-outs • View the **Print** button on the **Confirmation Summary** page • View and edit the **Profile** page on the **Admin** tab, where users can edit their profile information (view user details and change passwords)

© Copyright IBM Corporation. 2019.

IBM Confidential

Appointments with Opt-Out	IBM Phytel Remind	This role is for front office staff, schedulers, or practice managers and has the additional feature to "opt-out" (stop communication with) patients for various reasons. This feature is permission-based and can be given to specific users within your organization. Following are some actions these users can perform: • View patient responses to communications regarding their upcoming appointments on the **Confirmation Summary** page on the **Remind** tab • Search for patients using the **Patient Search** field • View the **Patient Summary** pop-up page, which lists historical patient communications and opt-outs • View the **Print** button on the **Confirmation Summary** page • View and edit the **Profile** page on the **Admin** tab, where users can edit their profile information (view user details and change passwords) • Access to the **Opt Out Settings** page on the **Patient Summary** pop-up page and permission to opt patients out of receiving IBM Phytel Remind communications ⚠ Users who would like appointments with opt-out permissions should only select **Appointments with Opt-Out** and not **Appointments** also.
Alert Notifications	IBM Phytel Remind	This role is typically for a practice manager and gives them the ability to create immediate and same-day phone communications to alert patients the office will be closed or that a provider is unavailable. • View and create alert notifications on the **Alert Notifications** page on the **Remind** tab
Outreach	IBM Phytel Outreach	This role is designed for any users who need to access the IBM Phytel Outreach application to determine the reason for which a patient was contacted. Primarily, these users are scheduling staff, but this role can be granted to anyone desiring to view the reason for an IBM Phytel Outreach communication. The role consists of the following: • View the **Outreach Summary** page on the **Outreach** tab • Search for patients using the **Patient Search** field • View the **Patient Summary** pop-up page, which lists historical patient communications and opt-outs • View the **Print** button on the **Confirmation Summary** page • View and edit the **Profile** page on the **Admin** tab, where users can edit their profile information (view user details and change passwords)
Outreach with Opt-Out	IBM Phytel Outreach	This role has the additional feature to "opt out" (stop communication with) patients for various reasons related to IBM Phytel Outreach. Following are some actions these users can perform: • View the **Outreach Summary** page on the **Outreach** tab • Search for patients using the **Patient Search** field • View the **Patient Summary** pop-up page, which lists historical patient communications and opt-outs • View the **Print** button on the **Confirmation Summary** page • View and edit the **Profile** page on the **Admin** tab, where users can edit their profile information (view user details and change passwords) • Access the **Opt Out Settings** page on the **Patient Summary** pop-up page, and opt patients out of receiving IBM Phytel Outreach communications. ⚠ Users who would like IBM Phytel Outreach with opt-out permissions should only select **IBM Phytel Outreach with Opt-Out** and not **IBM Phytel Outreach** also.
Insight and Dashboard (Insight)	IBM Phytel Coordinate	The **Insight** tab allows users to benchmark, trend, and analyze performance related to patient care. Executive Management, Medical Directors, Providers, Nurse Practitioners, Care Coordinators, Nurses, Practice Managers, Medical Assistants, and Schedulers use the **Insight** tab. This role allows users to view reports. Following are some actions these users can perform: • View the **Dashboard** page on the **Insight** tab • View the **Benchmark** page on the **Insight** tab • View the **Comparison** page on the **Insight** tab • View the **Population** page on the **Insight** tab • View care opportunities on the **Opportunities** page on the **Insight** tab • View the **Patients** page on the **Insight** tab • View and download reports on the **Reports** tab

© Copyright IBM Corporation. 2019.

IBM Confidential

Transition	IBM Phytel Transition	This role is designed for any users who might need to access the IBM Phytel Transition application to view patients who need follow-up. This role is typically assigned to a nurse whose job is to contact patients identified through the application as needing follow-up. It allows users to perform the following actions: • View the list of patients on the **Follow-up List** page • View the **Call Results** page • View the **Transition** tab • View and edit the **Profile** page on the **Admin** tab, where users can edit their profile information (view user details and change passwords)
Transition Opt Out	IBM Phytel Transition	This role lets a user turn off Transition phone calls for a patient who does not want to receive calls. Users can perform the following actions: View and edit the **Opt-Out** page on the **Transition** tab
Coordinate with Campaigns	IBM Phytel Coordinate	This role is is an additional capability within IBM Phytel Coordinate that provides users the ability to send patients a communication related to their health needs. Users can perform the following actions: • View the **Coordinate** tab • View and edit the **Patient Management** page on the **Coordinate** tab • Access the **Send Campaigns** button, which allows users to create campaigns • View the **Campaigns** page on the **Coordinate** tab. This allows users to view existing campaigns
Coordinate Reports	IBM Phytel Coordinate	This is the main role that gives users access to IBM Phytel Coordinate. It is typically designed for Schedulers, Medical Assistants, Practice Managers, Nurses, Care Managers, Physician Assistants, Nurse Practitioners, Quality team members, and Providers, giving users the following permissions: • View the **Coordinate** tab • View and edit the **Patient Management** page on the **Coordinate** tab
Coordinate Assign Care Manager_Me Only	IBM Phytel Coordinate	This role is an additional capability within IBM Phytel Coordinate that provides a user the ability to *only* assign himself or herself as the primary care manager of a patient.
Coordinate Assign Care Manager	IBM Phytel Coordinate	This role is an additional capability within IBM Phytel Coordinate that allows users to assign themselves or another individual as the primary care manager for a patient.
Coordinate Remove Care Manager Assignment	IBM Phytel Coordinate	This role is an additional capability within IBM Phytel Coordinate that allows users to remove themselves or an individual as the primary care manager for a patient.
Patient Summary	IBM Phytel Coordinate	This role is currently accessible only by clicking on a patient name on the **Coordinate Patient Management** page. The **Patient Summary** tab allows users to click on a specific patient in IBM Phytel Coordinate and see a snapshot of that patient with demographic and clinical information. Any IBM Phytel Coordinate user should also likely have this access. Following are some actions that users with this role can perform: • View the **Patient** tab, which displays the **Patient Summary** page, including the patient **Dashboard**, **Communication History**, and **Notes** • View **Alerts & Recommendations** • View and edit **Notes** on the **Patient Summary** page
Patient Summary with Data Limitation	IBM Phytel Coordinate	This role is a subset of **Patient Summary** permissions with a limit on data shown on the **Communication History** page by groups and providers the user has rights to. Following are some actions that users with this role can perform: • View the **Patient** tab • View the **Communication History** page on the **Patient Summary** page • View and edit the **Profile** page on the **Admin** tab, where users can edit their profile information (view user details and change passwords)

© Copyright IBM Corporation. 2019.

IBM Confidential

Coordinate Administrator	IBM Phytel Coordinate	This role provides Administrators access to the **Patient** tab with the ability to edit or remove **Patient Summary** notes, and access to the **Admin** tab for editing user profiles and editing IBM Phytel Coordinate product settings. Following are some actions that users with this role can perform: • Notes administration and sending page views to other users • Edit and remove notes from the **Patient Summary** page • View Coordinate **Campaign Addresses** admin page • View Coordinate **Notes Categories** admin page • View the **Patient** tab • View the **Products** page on the **Admin** tab • View Coordinate **Share Page Views** admin page • View and edit the **Profile** page on the **Admin** tab, where users can edit their profile information (view user details and change passwords)
Coordinate Share Page Views	IBM Phytel Coordinate	This role is an additional capability within IBM Phytel Coordinate that provides a user the ability to share with other users a saved view that has already been created in IBM Phytel Coordinate. Following are some actions a user with this role can perform: • Send **Page Views** to other users in the contract on the **Admin** tab • View the **Products** page using the **Admin** tab • View IBM Phytel Coordinate **Shared Page Views** on the **Admin** page • View and edit the **Profile** page on the **Admin** tab, where users can edit their profile information (view user details and change passwords) **Note** The patient results of a page view are not shared, but rather just the framework for the query.
Coordinate Note Categories	IBM Phytel Coordinate	This security role is an additional capability within IBM Phytel Coordinate that allows administrators to create, edit, and delete categories for the notes the care managers enter. Typically, this is a superuser, and the permission is not shared with others, as they have specific categories they need for reporting. **Note** These notes do not post-back to the EMR.
Reports	N/A	This role is assigned to specific users who need to view reports specific to their health system, such as quarterly IBM Phytel Outreach reports. Following are some actions these users can perform: • View and download value reports, ad hoc reports, measure details, campaign templates, and user guides on the **Reports** tab • View and edit the **Profile** page on the **Admin** tab, where users can edit their profile information (view user details and change passwords) If users have **Insight** or **Reports** permissions, then they can view the **Reports** tab.
Administrator	N/A	This role is typically provided to administrative users, because it allows an individual to add new users, delete users, assign security roles, reset passwords, and so on. Following are some actions these users can perform: View, create, and edit users on the **Profile** page, **Users** page, and **Products** page on the **Admin** tab. **Note** As an Administrator, you can only assign security roles that you have access to. To assign all security roles, you should also be assigned all security roles.
Single Sign on (SSO) Enabled	N/A	This role enables Single Sign on (SSO) on the **Admin** tab and is specific to users who have SSO enabled on their contract. There are no permissions required for this role.
Meaningful Use Reports	N/A	This role allows users to create meaningful use reports via the **Meaningful Use** page on the **Reports** tab.
Coordinate with Cohort Save	IBM Phytel Coordinate	This role allows users to view the **Cohort** page and to create and save cohorts within the user's health system. The saved cohort is then available in the **Patient Management** view's **Filtering** section.

© Copyright IBM Corporation. 2019.

IBM Confidential

Coordinate with Cohort Send	IBM Phytel Coordinate	This role allows users to view the **Cohort** page and to use the **Send Cohort** button on the **Cohorts** page (which makes a saved cohort available in IBM® Watson Care Manager).
Payer Subgroup Admin	IBM Phytel Coordinate	This role allows users to view the **Payor Subgroup** page and to create and save payor subgroups within the user's health system. The saved payor subgroup is then available in the **Patient Management** view's **Filtering** section when the **Payor Subgroup** item is selected.
NPS In-App Survey for Coordinate	IBM Phytel Coordinate	This role allows users to provide product feedback in the Net Promoter Score survey. It appears when the user accesses certain pages in the **Coordinate** or **Insight** tabs. **Recommendation** IBM recommends that administrators do not apply this role to users. This role allows users to see and respond to the Net Promoter Score survey with the intention that IBM will contact these respondents for more information.
NPS In-App Survey for Outreach	IBM Phytel Outreach	This role allows users to provide product feedback in the Net Promoter Score survey. It appears when the user accesses the **Outreach** tab. **Recommendation** IBM recommends that administrators do not apply this role to users. This role allows users to see and respond to the Net Promoter Score survey with the intention that IBM will contact these respondents for more information.
NPS In-App Survey for Remind	IBM Phytel Remind	This role allows users to provide product feedback in the Net Promoter Score survey. It appears when the user accesses certain pages in the **Remind** tab. **Recommendation** IBM recommends that administrators do not apply this role to users. This role allows users to see and respond to the Net Promoter Score survey with the intention that IBM will contact these respondents for more information.
QRDA Measures	IBM Phytel Coordinate	This role allows users to view and use the **Measures** page on the **Coordinate** tab. Use the **Measures** page to import QRDA I files and to export QRDA I and III files for reporting.
View Audit Report	N/A	This role allows users to view and use the **Audit Report** page on the **Admin** tab. Use the **Audit Report** page to view activity (including affected patients) for users. For more information, see

© Copyright IBM Corporation. 2019.

IBM Confidential

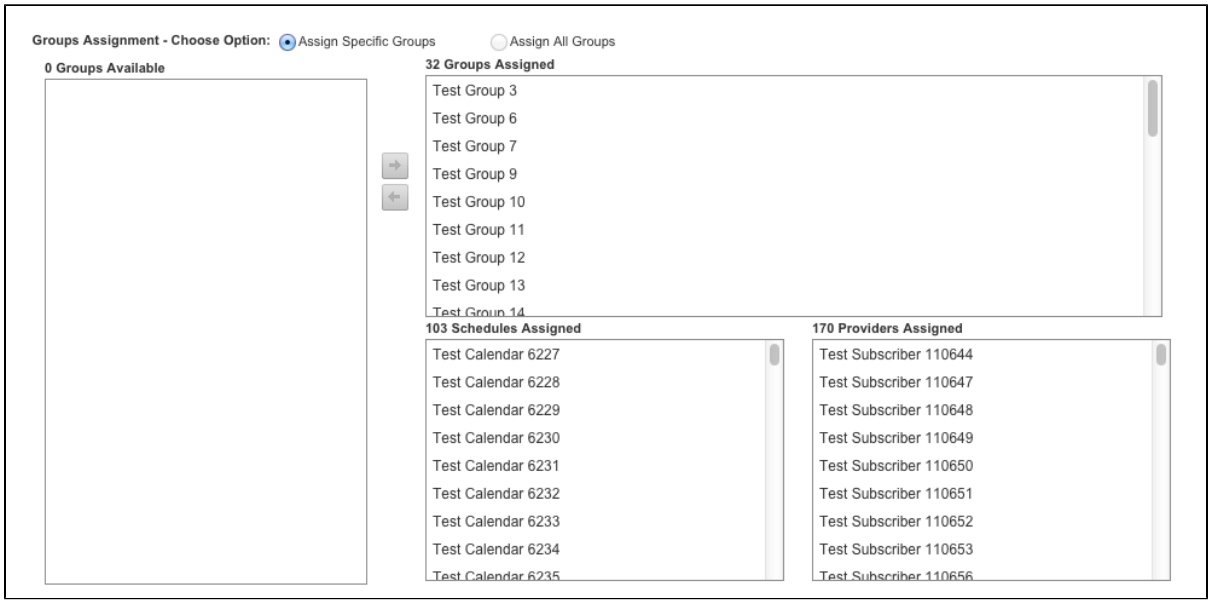
Assigning Groups

Groups are based on a collection of schedules or a collection of providers. Therefore, you must assign groups to a user if you want them to see patients. If no groups are assigned, the user's functionality would be limited to **Reports** and **Admin**, depending upon their assigned roles.

When creating or editing a user, you can assign groups to a user in the **Groups Assignment** area.

> **Groups available to be assigned**
>
> You can only assign groups that you are also assigned. However, you can remove groups that you are not assigned.

Groups Assignment Area of the Admin Tab



To assign groups to a user:

1. Ensure that **Assign Specific Group**s is selected.
   If you are creating a call center user, then select **Assign All Groups**; if the user is granted the **All Groups** option, then they have access when a new group is added.
2. Select the group(s) to assign to the user from the **Groups Available** box.

   > **Selecting More Than One Group**
   >
   > You can select more than multiple contiguous groups using the Shift+click method to click the first and last group you want to assign.

3. Click → to move the selected group(s) selected to the **Groups Assigned** box.

   Click ← if you want to move a group from the **Groups Assigned** box back to the **Groups Available** box.

   > **Schedules and Providers**
   >
   > After you move groups into the **Groups Assigned** box, the schedules and providers that are assigned to these groups display in the **Schedules Assigned** and **Providers Assigned** boxes.

4. Click **Save**.

© Copyright IBM Corporation. 2019.

IBM Confidential

Understanding Groups

Once assigned to a group, the user can access any schedules or providers that are associated to the group; thus, the user has access to the patients that are associated to the respective schedules and providers based on their group permissions.

The image below represents the following:

Three groups are set up:

- Group 1
- Group 2
- Group 3

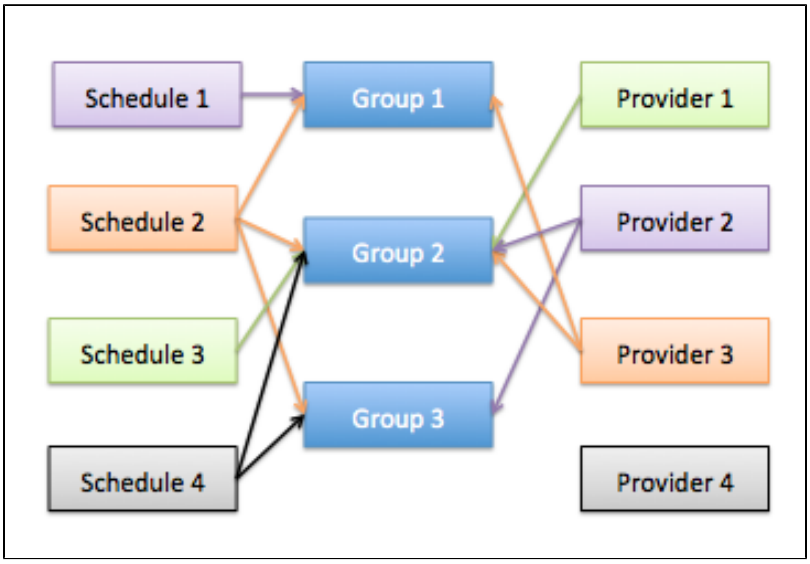
Four schedules are set up, and each is assigned to different groups:

- Schedule 1 is assigned to Group 1
- Schedule 2 is assigned to Group 1, Group 2, and Group 3
- Schedule 3 is assigned to Group 2
- Schedule 4 is assigned to Group 2 and Group 3

Four providers are set up, and all but one are assigned to at least one group:

- Provider 1 is assigned to Group 2
- Provider 2 is assigned to Group 2 and Group 3
- Provider 3 is assigned to Group 2
- Provider is not assigned to any group

Example of Group Assignment



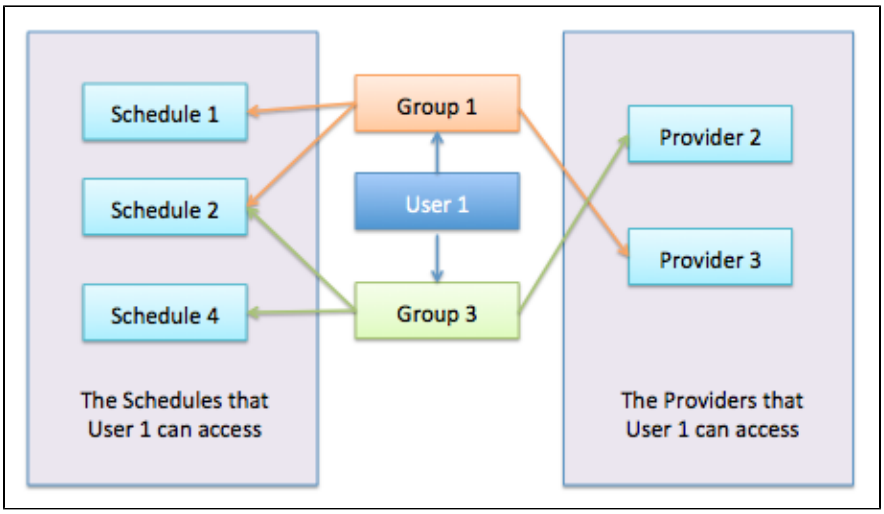
When you assign one or more of these groups to a user, that user has the groups' associated schedules and providers.

In the example below, User 1 is given permission to Group 1 and Group 3.

Example of User Assigned to Two Groups

© Copyright IBM Corporation. 2019.

IBM Confidential



Because of User 1's group permission, User 1 also has permission to Schedule 1, Schedule 2, and Schedule 4, as well as permission to Provider 2 and Provider 3. Therefore, User 1 can access patient information associated with any of the following:

- Schedule 1
- Schedule 2
- Schedule 4
- Provider 2
- Provider 3

Other restrictions around the content the user has access, based on groups, include:

- Only active groups that have associated, enabled schedules are visible in IBM Phytel Remind.
- Only active groups that have associated, enabled providers are visible in IBM Phytel Outreach.
- Only active groups that have providers that are associated with a quality initiative are visible in the **Insight** tab in IBM Phytel Coordinate.
- Only active groups that have providers enabled for IBM Phytel Coordinate are visible in IBM Phytel Coordinate.
- The user can only search patients associated with schedules and providers associated with groups that the user has access to.

© Copyright IBM Corporation. 2019.

IBM Confidential

Hospital and Unit Access

Hospitals are used within IBM Phytel Transition, and each hospital may be associated with one or more units. The hospital-unit combination is also associated with a group. Therefore, a user may access only those hospital-unit combinations that are associated to groups that they are assigned. Only those hospitals and associated units are visible to the user within IBM Phytel Transition.

© Copyright IBM Corporation. 2019.

IBM Confidential

Schedule Access Exceptions

Regardless of whether a schedule is associated with a group, and a user is assigned to that group, if that schedule is not turned on, then the user will not see it as an option in any **Schedule** list. Therefore, any patients associated with only that schedule and no other schedules will be inaccessible within the application.

© Copyright IBM Corporation. 2019.

IBM Confidential

Provider Access Exceptions

Regardless of whether a provider is associated with a group, and a user is assigned to that group, other requirements must be met before the provider is accessible in each of the products:

- For IBM Phytel Outreach, the provider must only be enabled.
- For IBM Phytel Coordinate, the provider must be enabled for the IBM Phytel Coordinate product.
- For the **Insight** tab, the provider must be associated with at least one quality initiative.

Patients associated with providers not visible in the respective products are inaccessible when using those products or their date included in any page content that the user is accessing within those products.

© Copyright IBM Corporation. 2019.

IBM Confidential

Creating Audit Reports of User Activity

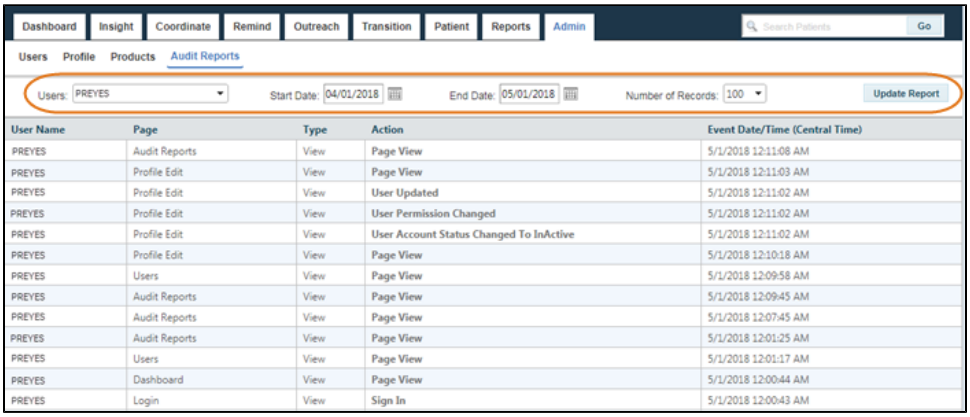
You can create an audit report for a specific time for selected users. From this report, you might review user's actions, which include changes, deletions, additions, access, and queries. You might also view the patients whose data was involved in an action.

You must have the View Audit Report security role to use the **Audit Reports** section.

You can view audit reports only for the users who are assigned to you. You cannot view reports for users who are assigned to other administrators.

1. In the **Admin** tab, click the **Audit Reports** section.
2. Select one or more users, a start and end date for the report, and the number of actions to show.
   You are limited to viewing only 500 of the most recent user activities.

> **Tip**
>
> By default, all users are selected. If you select a specific user but then want to select all users, clear all selected users. All users are selected automatically.



3. Click **Update Report** to show a history of activities in IBM Phytel for the selected users.

> **Note**
>
> When you change the users, the start and end dates, or the number of records, you must click **Update Report** to show the results.

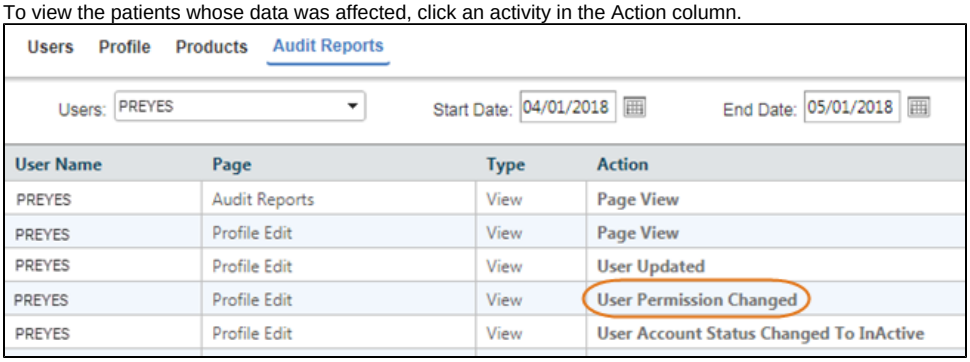
4. Click a column heading to sort the list on the values in that column.

Column	Description
User Name	The name of the selected user.
Page	The page of the IBM Phytel application where a user acted. The Page column does not show the names of specific dialog boxes that a user accessed.
Type	The type of action that a user took. The available action types are View, Export, Import, Delete, and Insert. You can use this column to sort user actions to focus on specific types. For example, you might want to look only at Delete actions.
Action	The specific action that a user took. You might see an action that differs from the Type. For example, an action has a View type, though the action was User Permission Changed. The reason is that the page has a dialog box that opens, which is where the user acted, such as changing permissions.

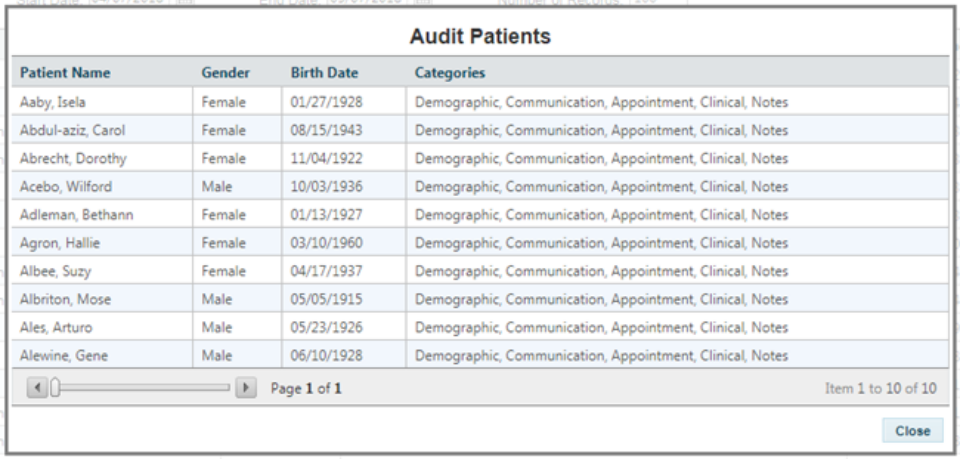
© Copyright IBM Corporation. 2019.

IBM Confidential

5. To view the patients whose data was affected, click an activity in the Action column.



6. In the Audit Patients window, review the list of patients.
   The Categories column shows the category that the action belongs to. An action can fall into multiple categories.
   Some actions might not list any patients because no patient data was displayed or modified, such as a Page View action.



© Copyright IBM Corporation. 2019.

IBM Confidential

Notices

This information was developed for products and services offered in the US.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.
This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

© Copyright IBM Corporation. 2019.

IBM Confidential

Trademarks

IBM, the IBM logo, IBM Phytel, IBM Phytel Coordinate, IBM Phytel Transition, IBM Phytel Outreach, IBM Phytel Remind, IBM Phytel Engage, the Phytel logo, and combinations thereof are trademarks of IBM Corporation, registered in many jurisdictions worldwide.

Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.