SPHER

User Guide

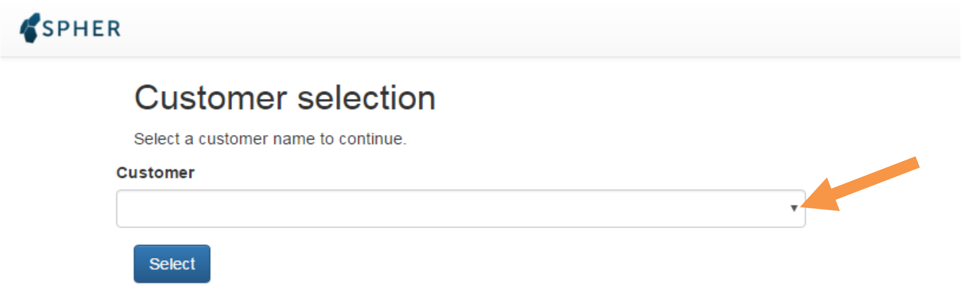
UPDATED: 9/1/2017

Contents

1_Multiple Customer Accounts

Overview: For SPHER clients that oversee more than one Customer Account, e.g., a hospital network that uses SPHER on behalf of private practices and clinics under their management, **Customer Selection** is prompted upon logging in. However, for most SPHER clients this screen will not be available upon logging in.

Should you be prompted with the Customer Selection Screen, use the dropdown menu to select the customer you wish to view.

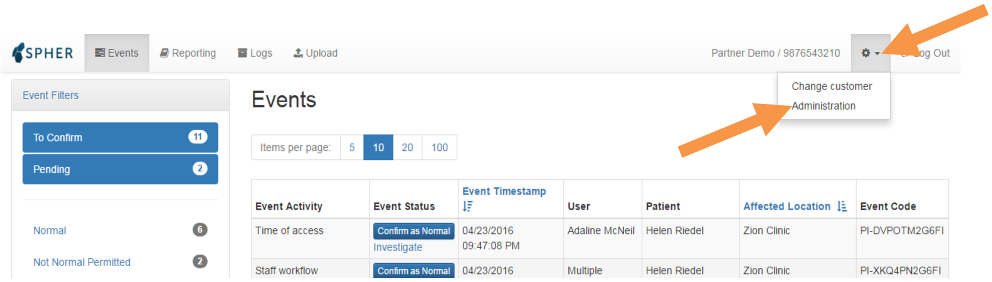


Customer selection

Select a customer name to continue.

Customer

Alternatively, there is a section of the upper-right corner of your screen that displays the **Customer Name**/**Customer Code** currently selected as well as a **"Gear" icon** that can be used to change customer accounts. This "Gear" icon is available on all pages of SPHER for ease of account switching. Click the "**Gear" icon** then click **Change Customer** from the dropdown menu to switch to another Customer Account.



Partner Demo / 9876543210

Events

Event Activity	Event Status	Event Timestamp	User	Patient	Affected Location	Event Code
Time of access	Confirm as Normal Investigate	04/23/2016 09:47:08 PM	Adaline McNeil	Helen Riedel	Zion Clinic	PI-DVPOTM2G6FI
Staff workflow	Confirm as Normal	04/23/2016	Multiple	Helen Riedel	Zion Clinic	PI-XKQ4PN2G6FI

2_Managing Users

Overview: SPHER allows SPHER users to have a variety of SPHER access permissions. These permissions are managed by SPHER users who have Administration privleges. If you do not see the Administration link in the dropdown menu that appears after clicking on the “Gear” icon in the upper right-hand corner, you do not have Administration privileges. A SPHER Administrator can do the following:

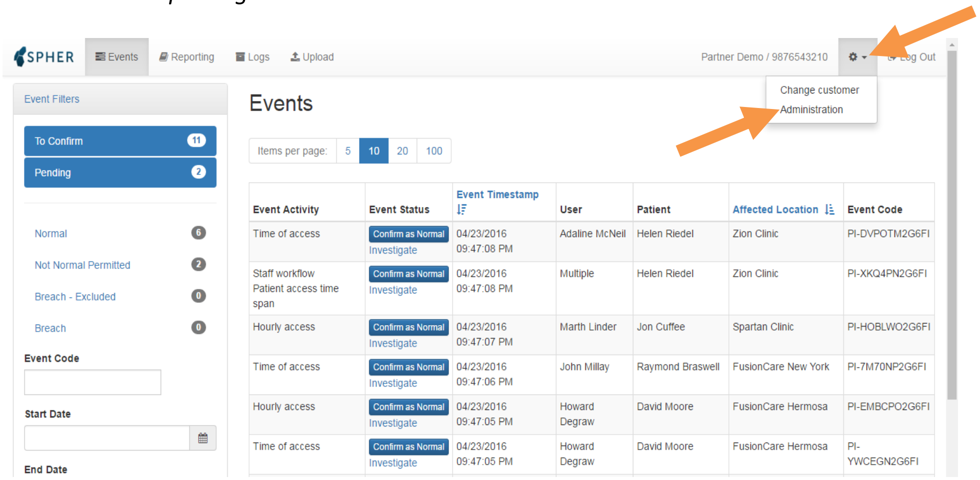
- Change the permissions of current users
- Add a new user or disable a current user

To change user permissions, follow the steps below:

Step 1: Go to **dashboard.amsspher.com** and log in to your SPHER account.

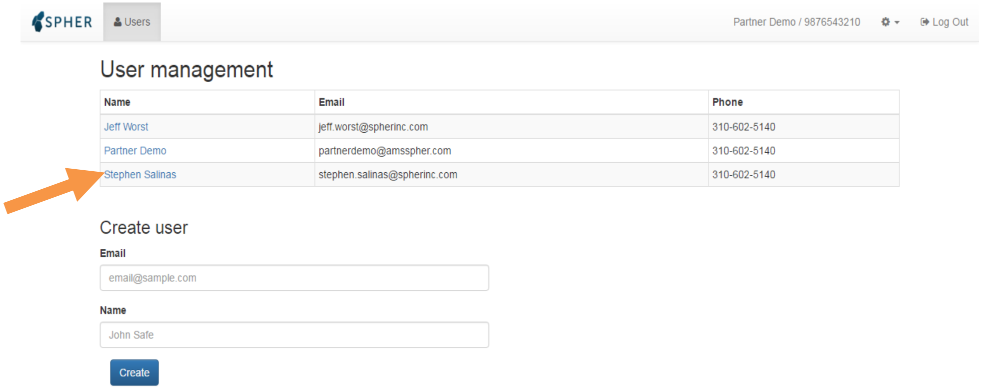
Step 2: Click on the **“Gear” icon** located at the top right of your screen. A dropdown menu will appear. Click **Administration**.

Note: *The Administration link will not appear in the dropdown menu if the user does not have Administration privileges.*



Event Activity	Event Status	Event Timestamp	User	Patient	Affected Location	Event Code
Time of access	Confirm as Normal Investigate	04/23/2016 09:47:08 PM	Adaline McNeil	Helen Riedel	Zion Clinic	PI-DVPOTM2G6FI
Staff workflow Patient access time span	Confirm as Normal Investigate	04/23/2016 09:47:08 PM	Multiple	Helen Riedel	Zion Clinic	PI-XKQ4PN2G6FI
Hourly access	Confirm as Normal Investigate	04/23/2016 09:47:07 PM	Marth Linder	Jon Cuffee	Spartan Clinic	PI-HOBLWO2G6FI
Time of access	Confirm as Normal Investigate	04/23/2016 09:47:06 PM	John Millay	Raymond Braswell	FusionCare New York	PI-7M70NP2G6FI
Hourly access	Confirm as Normal Investigate	04/23/2016 09:47:05 PM	Howard Degraw	David Moore	FusionCare Hermosa	PI-EMBCPO2G6FI
Time of access	Confirm as Normal Investigate	04/23/2016 09:47:05 PM	Howard Degraw	David Moore	FusionCare Hermosa	PI-YWCEGN2G6FI

Step 3: Click the **User Name** you want to manage from the list to access the **User Details page**.



User management

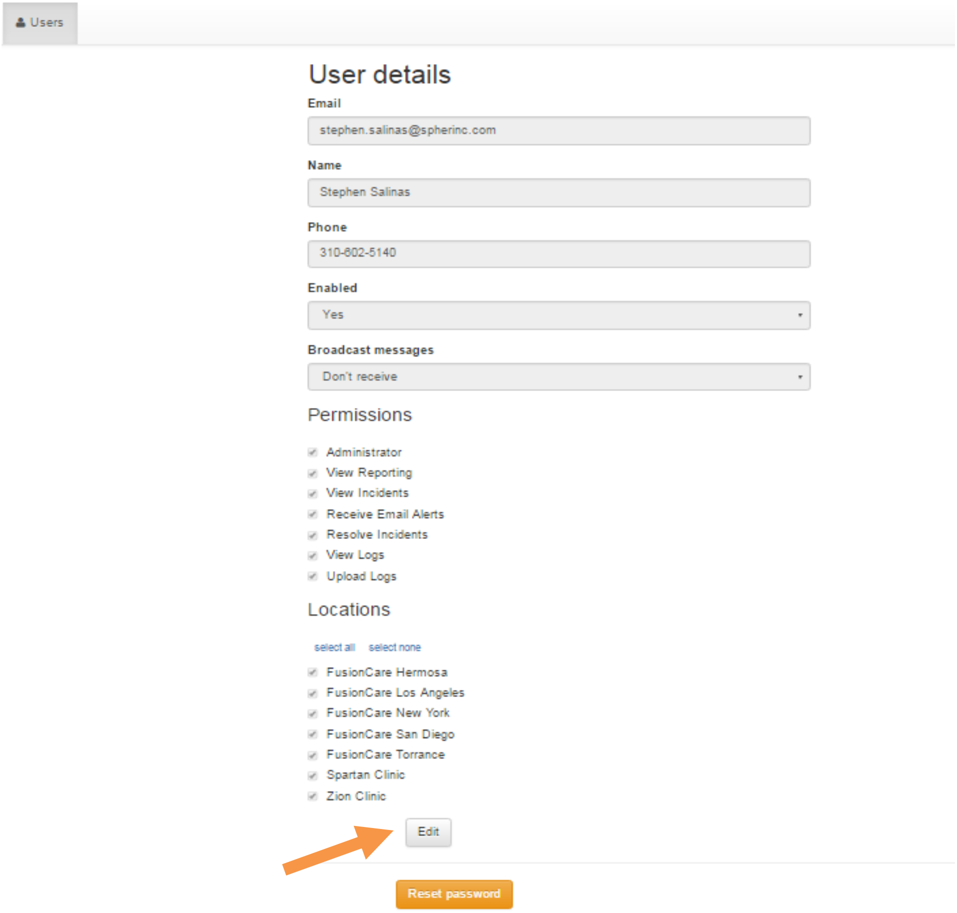
Name	Email	Phone
Jeff Worst	jeff.worst@spherinc.com	310-602-5140
Partner Demo	partnerdemo@amsspher.com	310-602-5140
Stephen Salinas	stephen.salinas@spherinc.com	310-602-5140

Create user

Email: email@sample.com

Name: John Safe

Step 4: Click **Edit** at the bottom of the page and select the desired settings for this user. An explanation of the SPHER permissions that an Administrator can set for each SPHER user are outlined in a following section of this guide, *2.2_User Permissions*.



User details

Email: stephen.salinas@spherinc.com

Name: Stephen Salinas

Phone: 310-602-5140

Enabled: Yes

Broadcast messages: Don't receive

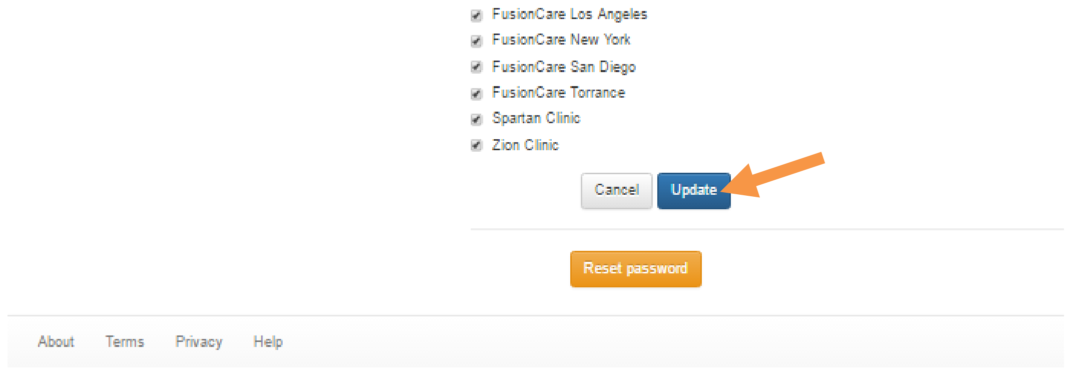
Permissions

- ☑ Administrator
- ☑ View Reporting
- ☑ View Incidents
- ☑ Receive Email Alerts
- ☑ Resolve Incidents
- ☑ View Logs
- ☑ Upload Logs

Locations

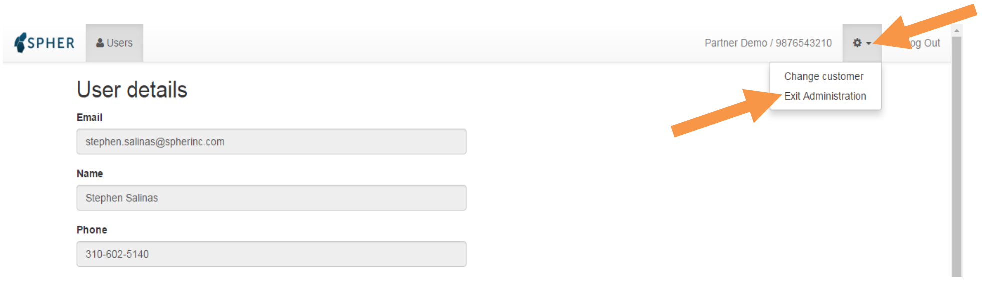
- ☑ FusionCare Hermosa
- ☑ FusionCare Los Angeles
- ☑ FusionCare New York
- ☑ FusionCare San Diego
- ☑ FusionCare Torrance
- ☑ Spartan Clinic
- ☑ Zion Clinic

Step 5: Click **Update** at the bottom of the page to save any changes made to a user's SPHER permissions.



☑ FusionCare Los Angeles
☑ FusionCare New York
☑ FusionCare San Diego
☑ FusionCare Torrance
☑ Spartan Clinic
☑ Zion Clinic

Step 6: To go back to the Dashboard, click on the **"Gear" icon** located at the top right of your screen. A dropdown menu will appear. Click **Exit Administration**.



User details

Email
stephen.salinas@spherinc.com

Name
Stephen Salinas

Phone
310-602-5140

2.1_Setting User Permissions

Overview: A SPHER Administrator can set a number of permissions for individual SPHER users that allow or restrict access individual pages within SPHER, allow or restrict access to various locations within an organization, deactivate users that no longer need access, or reset user passwords.

Below is an explanation of the SPHER permissions and user settings that an Administrator can set for each SPHER user:

Enabled – determines if a SPHER user is or is not able to log into the SPHER dashboard (e.g., deactivating a user who no longer needs access to SPHER).

Broadcast Messages – determines if a user will receive emails sent to all SPHER users at the same time (e.g., announcement of a new version of SPHER soon to be released).

Permissions

- Administrator –add/disable users and modify user permissions and settings
- View Reporting – access the Reporting page
- View Events – view the Events page (cannot resolve events, view only)
- Receive Email Alerts – receive emails when an event is detected by SPHER
- Resolve Events – view the Events page and ability to resolve events
- View Logs – access to the Logs page
- Upload Logs – access to Upload page

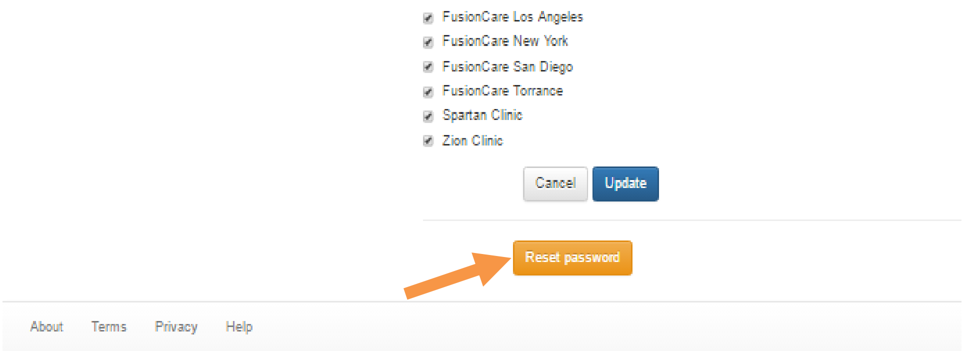
Locations

The Administrator can select from which location(s) a user has permission to:

- Receive event email alerts
- View and resolve events
- View log records

Reset Password

If a user forgets their password, clicking the “Reset Password” button sends the user an email with a link for resetting his or her password. The email link is only valid for 24 hours from the time it was sent.



☑ FusionCare Los Angeles
☑ FusionCare New York
☑ FusionCare San Diego
☑ FusionCare Torrance
☑ Spartan Clinic
☑ Zion Clinic

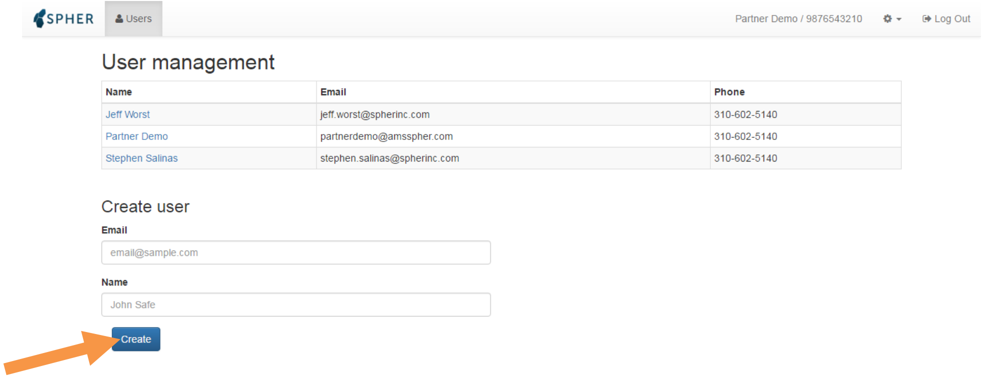
2.2_Creating New Users

Overview: A SPHER Administrator can add new SPHER users to their SPHER customer account by following the steps below:

Step 1: Go to **dashboard.amsspher.com** and log in to your SPHER account.

Step 2: Click on the **"Gear" icon** located at the top right of your screen. A dropdown menu will appear. Click **Administration**.

Step 3: Under the **Create User** section, enter the email address and the name of the user you want to add and then click **Create**.



User management

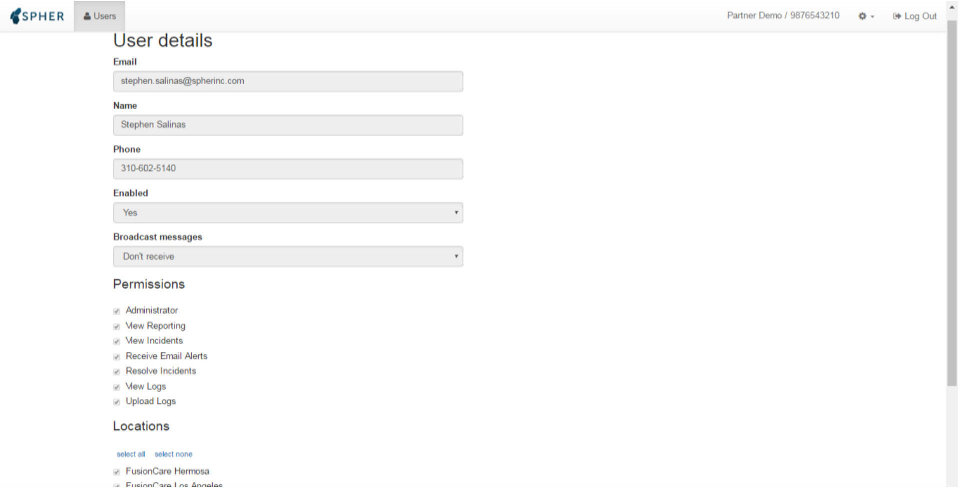
Name	Email	Phone
Jeff Worst	jeff.worst@spherinc.com	310-602-5140
Partner Demo	partnerdemo@amsspher.com	310-602-5140
Stephen Salinas	stephen.salinas@spherinc.com	310-602-5140

Create user

Email: email@sample.com

Name: John Safe

Step 4: Upon creating the new user, you will be taken to the **User Details** page where you can select the user settings and locations(s) this user has permissions to.



User details

Email: stephen.salinas@spherinc.com

Name: Stephen Salinas

Phone: 310-602-5140

Enabled: Yes

Broadcast messages: Don't receive

Permissions

- ☑ Administrator
- ☑ View Reporting
- ☑ View Incidents
- ☑ Receive Email Alerts
- ☑ Resolve Incidents
- ☑ View Logs
- ☑ Upload Logs

Locations

- ☑ FusionCare Hermosa
- ☑ FusionCare Los Angeles

Step 5: Upon creating the new user, the new user will sent an email with a link for setting his or her password for the first time. The email link is only valid for 24 hours from the time it was sent. Should the user fail to set a password in 24 hours and the link expires, the user's password will need to be reset. Instructions regarding Reset Password are outlined in a previous section of this guide, 2.1_Setting User Permissions.

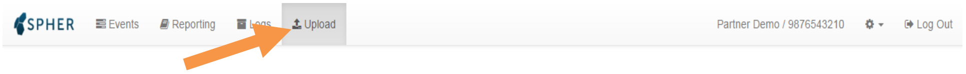
3_Uploading Audit Logs

Overview: SPHER uses the audit log files generated from your EHR/information system to analyze for irregular user activity. It is recommended that these audit log files be updated daily (previous 24 hours of activity) in order for SPHER to better accurately track for changes to the EHR user's behavior profile.

Note: *Some EHR systems allow for automation of audit log uploading on a daily basis. For EHR systems that allow for this functionality, this section of the guide is not applicable.*

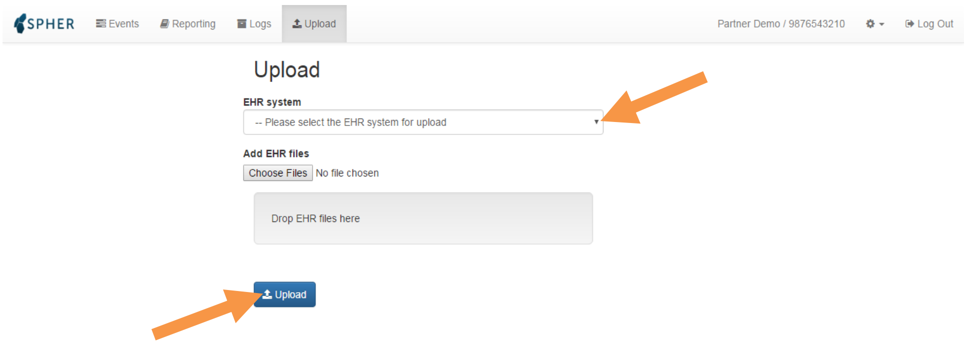
Step 1: Go to **dashboard.amsspher.com** and log in to your SPHER account

Step 2: To navigate to the **Upload page**, click the **Upload tab** at the top of your screen.



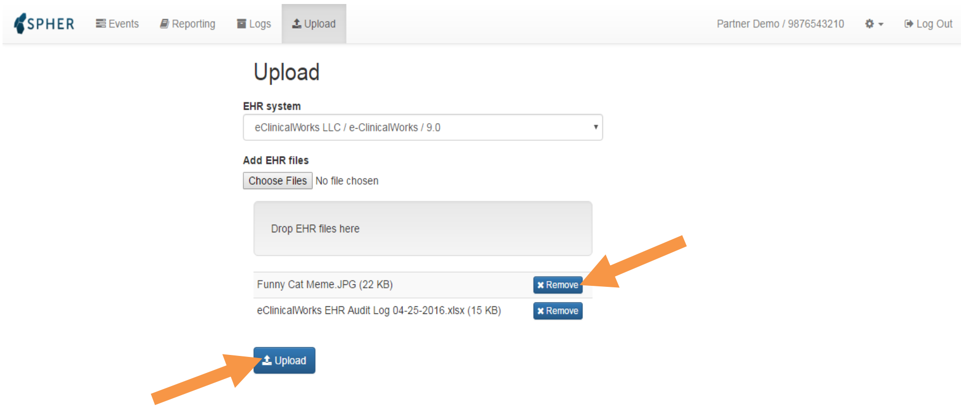
Step 3: Select the EHR/information system name from the dropdown list. Next, under "Add EHR files," click the **Choose Files button** and locate the audit log file from your computer. Alternatively, you may find it easier to drag and drop the files into the **"Drop Files Here" box**.

If you have multiple EHRs/information systems, you may upload multiple audit log files simultaneously. The maximum file size allowed for upload is 100 MB.



Step 4: Files that you have added will appear on the list below the "Drop Files Here" box. To upload, click the **Upload** button.

Note: *If a file was added to the upload list in error, you may remove it by clicking the* ***Remove button*** *on the right of the file name.*



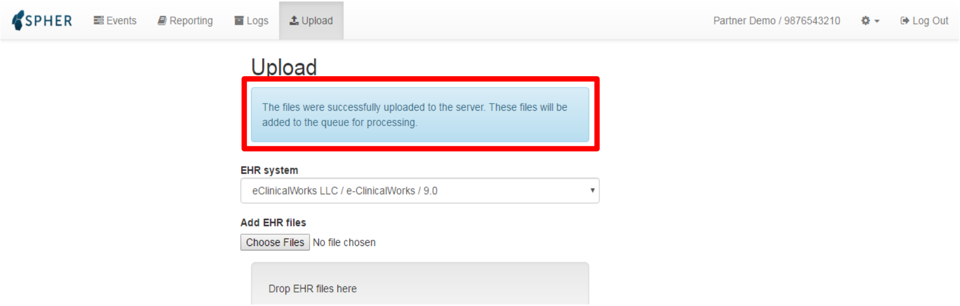
EHR system: eClinicalWorks LLC / e-ClinicalWorks / 9.0

Add EHR files: No file chosen

Funny Cat Meme.JPG (22 KB)

eClinicalWorks EHR Audit Log 04-25-2016.xlsx (15 KB)

Step 5: Verify the upload was successful. A validation message is displayed on the page that says: **“The files were successfully uploaded to the server. These files will be added to the queue for processing.”**



Upload

The files were successfully uploaded to the server. These files will be added to the queue for processing.

EHR system
eClinicalWorks LLC / e-ClinicalWorks / 9.0

Add EHR files
Choose Files No file chosen

Drop EHR files here

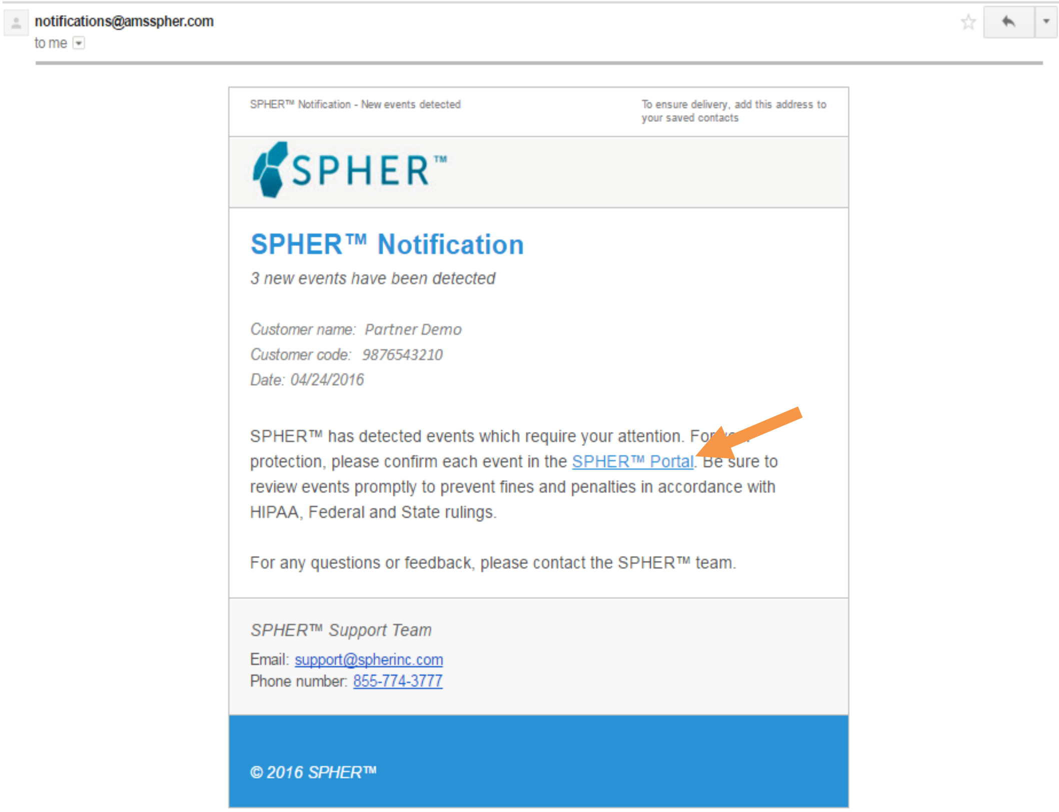
Note: *Audit logs will appear on the* ***Logs page*** *after they are processed. Processing time is approximately 24 to 48 hours. If you received an upload error notification in your email, contact SPHER Inc. at 855-774-3777 or email support@amsspher.com.*

4_Event Notification

Overview: When SPHER detects irregular user activities in the audit logs, SPHER will send you an **Alert** via an **Event Notification email**. These events will need to be investigated and resolved by logging in to SPHER.

Below is an example of an Event Notification email.

Note: A ***SPHER Portal*** *link is provided in the email for ease of access into SPHER.*



notifications@amsspher.com
to me

SPHER™ Notification - New events detected

To ensure delivery, add this address to your saved contacts

SPHER™

SPHER™ Notification

3 new events have been detected

Customer name: Partner Demo
Customer code: 9876543210
Date: 04/24/2016

SPHER™ has detected events which require your attention. For your protection, please confirm each event in the SPHER™ Portal. Be sure to review events promptly to prevent fines and penalties in accordance with HIPAA, Federal and State rulings.

For any questions or feedback, please contact the SPHER™ team.

SPHER™ Support Team
Email: support@spherinc.com
Phone number: 855-774-3777

© 2016 SPHER™

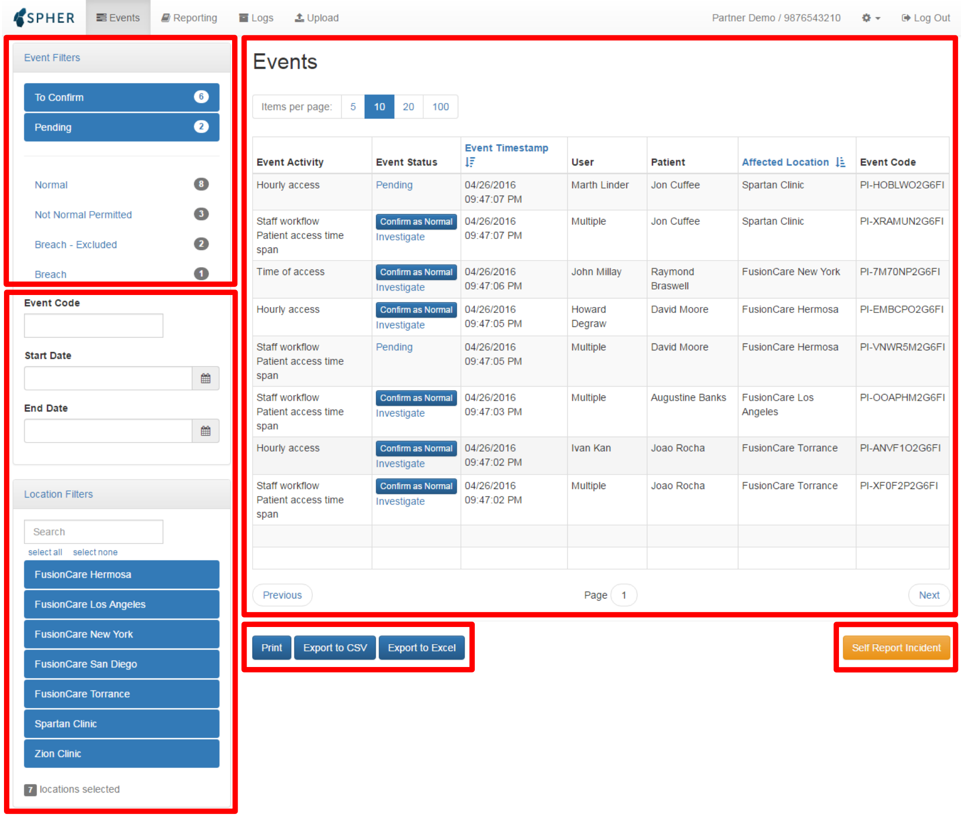
5_Events Page

Overview: The Events page is where you can find all the irregular user activities SPHER has detected in the audit logs. The Events page displays both new security events that require your immediate investigation as well as previously investigated and resolved events that are stored for your records as required by HIPAA. Various filters are also found on the events page. These filters allow a user to sort by event status, date range, and location (for organizations with multiple locations and/or departments). Users are also able to export event reports as well as self-report an incident on the Events page.

***Note:** For SPHER users with permissions to view the Events page, this page will open by default upon logging in.*

This section of the guide will provide an overview of the following features and functions of the Events page:

- Events Table
- Event Status Filters
- Location/Date Range/Event Code Filters
- Exporting Event Reports
- Self-Reporting Incident



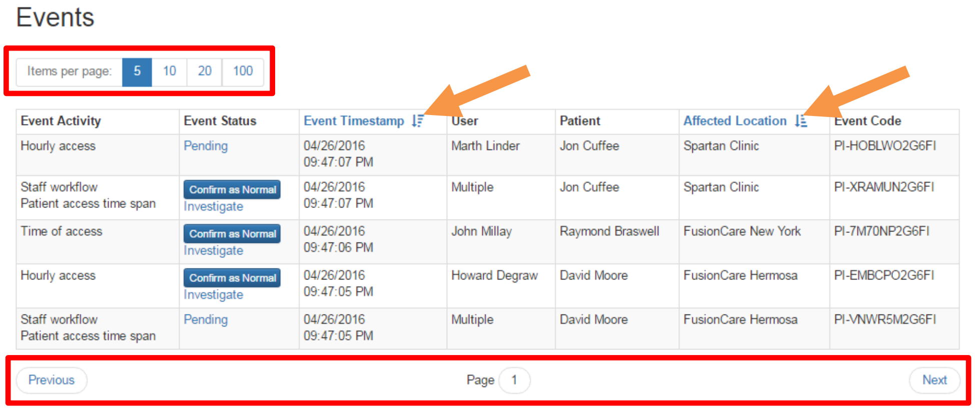
Event Activity	Event Status	Event Timestamp	User	Patient	Affected Location	Event Code
Hourly access	Pending	04/26/2016 09:47:07 PM	Marth Linder	Jon Cuffee	Spartan Clinic	PI-HOBLWO2G6FI
Staff workflow Patient access time span	Confirm as Normal Investigate	04/26/2016 09:47:07 PM	Multiple	Jon Cuffee	Spartan Clinic	PI-XRAMUN2G6FI
Time of access	Confirm as Normal Investigate	04/26/2016 09:47:06 PM	John Millay	Raymond Braswell	FusionCare New York	PI-7M70NP2G6FI
Hourly access	Confirm as Normal Investigate	04/26/2016 09:47:05 PM	Howard Degraw	David Moore	FusionCare Hermosa	PI-EMBCPO2G6FI
Staff workflow Patient access time span	Pending	04/26/2016 09:47:05 PM	Multiple	David Moore	FusionCare Hermosa	PI-VNWR5M2G6FI
Staff workflow Patient access time span	Confirm as Normal Investigate	04/26/2016 09:47:03 PM	Multiple	Augustine Banks	FusionCare Los Angeles	PI-OOAPHM2G6FI
Hourly access	Confirm as Normal Investigate	04/26/2016 09:47:02 PM	Ivan Kan	Joao Rocha	FusionCare Torrance	PI-ANVF1O2G6FI
Staff workflow Patient access time span	Confirm as Normal Investigate	04/26/2016 09:47:02 PM	Multiple	Joao Rocha	FusionCare Torrance	PI-XF0F2P2G6FI

5.1_Events Table

Overview: The Events Table shows you a list of all the events detected by SPHER.

Navigating the events table can be done in a number of ways. At the upper-left corner of the events table, you can select the number of events per page that you would like to view. At the bottom of the events table you can use the buttons to skip pages; the page number can also be found at the bottom. You can also sort the list in ascending/descending order by Event Timestamp and Location Name.

Note: *Events in the Events table are sorted in ascending order by Event Timestamp by default.*



Events

Items per page: 5 10 20 100

Event Activity	Event Status	Event Timestamp	User	Patient	Affected Location	Event Code
Hourly access	Pending	04/26/2016 09:47:07 PM	Marth Linder	Jon Cuffee	Spartan Clinic	PI-HOBLWO2G6FI
Staff workflow Patient access time span	Confirm as Normal Investigate	04/26/2016 09:47:07 PM	Multiple	Jon Cuffee	Spartan Clinic	PI-XRAMUN2G6FI
Time of access	Confirm as Normal Investigate	04/26/2016 09:47:06 PM	John Millay	Raymond Braswell	FusionCare New York	PI-7M70NP2G6FI
Hourly access	Confirm as Normal Investigate	04/26/2016 09:47:05 PM	Howard Degraw	David Moore	FusionCare Hermosa	PI-EMBCPO2G6FI
Staff workflow Patient access time span	Pending	04/26/2016 09:47:05 PM	Multiple	David Moore	FusionCare Hermosa	PI-VNWR5M2G6FI

Previous Page 1 Next

There are 7 columns within the events table that provide high level information for each detected event:

- Event Activity – the name of the activity detector that detected the event

  Note: *For more information refer to section 8_Concept Overview: Activity Detectors*
- Event Status – the current status of the event

  Note: *For more information refer to section 6_Concept Overview: Event Statuses*
- Event Timestamp – the time the event occurred
- User – the name of the individual who accessed the patient record
- Patient – the name of the patient whose record was accessed
- Affected Location – the location/department where the event occurred
- Event Code – a SPHER generated unique code given to each event

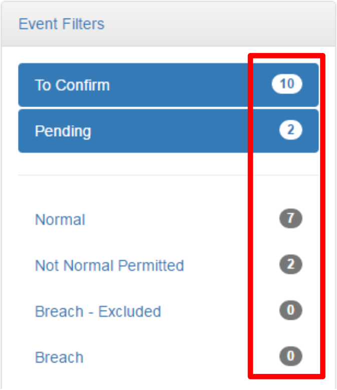
5.2_Event Status Filters

Overview: The event status filters are used to filter what is viewable on the Events table.

Upon log in, event statuses “To Confirm” and “Pending” are selected (as shown highlighted in blue) as these statuses represent events that require your attention and further investigation. Alternatively, events that have been previously been resolved (as shown not highlighted in blue) are not selected.

Next to each event status is a counter that shows the number of events that represented in each event status. In the event that either Location or Date Range Filters are selected, this number can change to reflect these filters being selected.

Note: *For more information and definitions for Event Statuses, see the following section of this guide, 6_Concept Overview: Event Statuses.*



5.3_Location/Date Range/Event Code Filters

Overview: The Events table can also be filtered by Locations and Date Range. SPHER users can also search for an event by entering a specific Event Code.

Should a user choose to filter by specific locations, the selections made will affect the events displayed in the Events table. Likewise, the counters next to each event status in the Event Filters sidebar will also change to reflect you location selection. Quick selection options for locations exist should a user want to select all or select none or search for the name of an individual location.

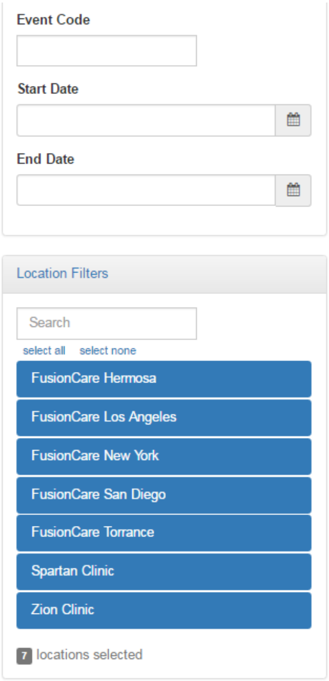
> ***Note:*** *Locations can represent separate offices of a medical group or separate departments within a hospital system.*

Users can also specify a specific date range by selecting a start and end date. Clicking the calendar icon located to the right of the Start and End Date text fields will open a date selection popup. The Event table and counters for each event status will change to reflect your selection.

> ***Note:*** *By default, the Start and End Dates are not specified, therefore the Event table will display ALL events detected by SPHER. If you have previously selected a date range but wish to revert back to viewing ALL detected events, you will need to delete the dates within the Start and End Date text fields.*

As indicated in the events table, each event is given a unique Event Code. Users can search specifically for an event by typing the unique code into the Event Code text field.

> ***Note:*** *If you have previously searched for an event by entering an Event Code and wish to revert back to viewing ALL detected events, you will need to delete the code within the Event Code text field.*



FusionCare Hermosa
FusionCare Los Angeles
FusionCare New York
FusionCare San Diego
FusionCare Torrance
Spartan Clinic
Zion Clinic

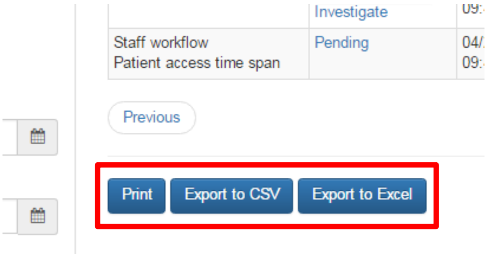
7 locations selected

5.4_Exporting Event Reports

Overview: Users are given the ability to quickly export reports containing the events displayed in the Events table at any time.

The options available to a user to export a report are Print, CSV, and Excel. Prior to exporting a report, users should select any filtering options they wish to be reflected. Exporting a file to either CSV or Excel allows users to further sort through any events detected by SPHER (e.g., filtering events detected from a specific user or involve a specific patient).

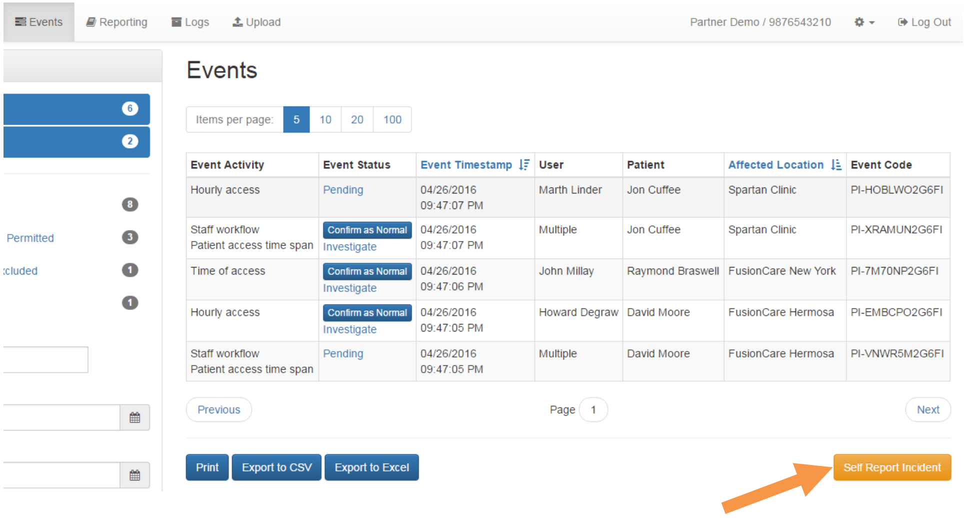
Note: *Event Reports generated on the Events page contain limited information when compared to the Event Reports generated on the Reporting page (i.e., Date Discovered and Resolution Date). For more information on event reports generated on the Reporting page, see the following section of this guide, 11_Reporting Page.*



5.5_Self-Reporting an Incident

Overview: SPHER allows you to document security incidents that may occur outside of user activity within an EHR/information system, such as a stolen laptop or missing hard drive. This feature enables a medical group to use SPHER as a central repository for all security incidents in order to meet documentation retention requirements under HIPAA. Similar to events detected by SPHER that require further investigation, incidents that are self-reported require a specific workflow to be followed in order to be resolved.

Step 1: Click on the **Self Report Incident** button on the bottom right corner below the Events table. This will take you to the **Self Report Incident page**.



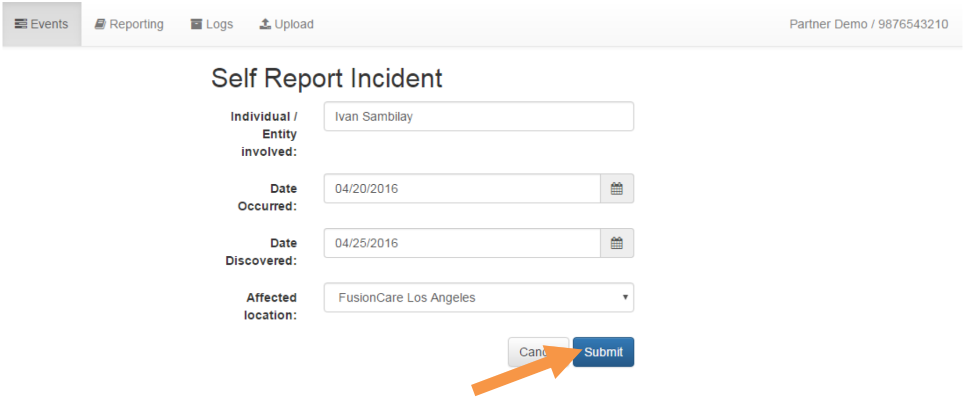
Events

Items per page: 5 | 10 | 20 | 100

Event Activity	Event Status	Event Timestamp	User	Patient	Affected Location	Event Code
Hourly access	Pending	04/26/2016 09:47:07 PM	Marth Linder	Jon Cuffee	Spartan Clinic	PI-HOBLWO2G6FI
Staff workflow Patient access time span	Confirm as Normal Investigate	04/26/2016 09:47:07 PM	Multiple	Jon Cuffee	Spartan Clinic	PI-XRAMUN2G6FI
Time of access	Confirm as Normal Investigate	04/26/2016 09:47:06 PM	John Millay	Raymond Braswell	FusionCare New York	PI-7M70NP2G6FI
Hourly access	Confirm as Normal Investigate	04/26/2016 09:47:05 PM	Howard Degraw	David Moore	FusionCare Hermosa	PI-EMBCPO2G6FI
Staff workflow Patient access time span	Pending	04/26/2016 09:47:05 PM	Multiple	David Moore	FusionCare Hermosa	PI-VNWR5M2G6FI

Previous Page 1 Next

Step 2: Enter the details of the incident in appropriate fields, and click **Submit**. This will create a new event with a status of "Pending."



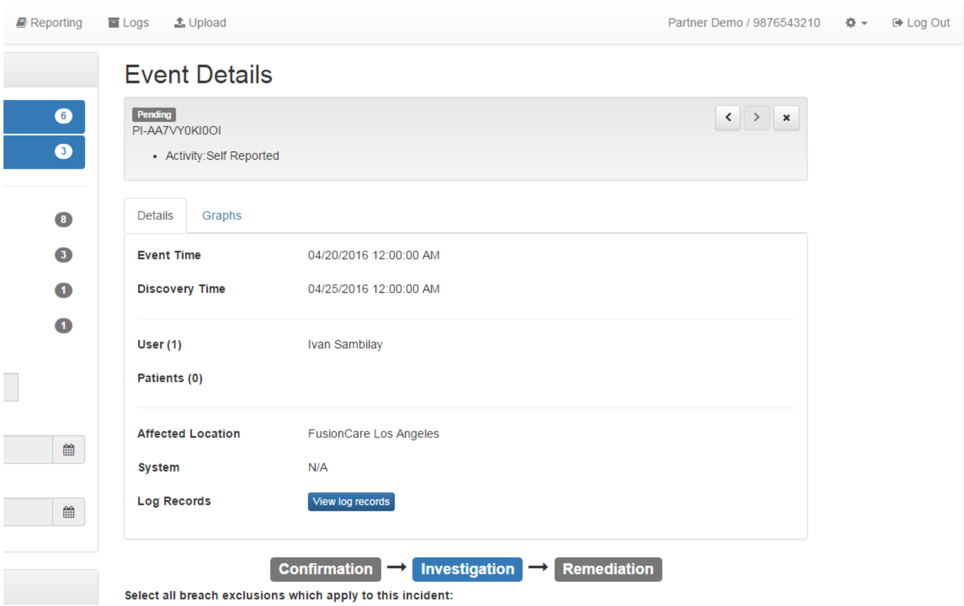
Self Report Incident

Individual / Entity involved:	Ivan Sambilay
Date Occurred:	04/20/2016
Date Discovered:	04/25/2016
Affected location:	FusionCare Los Angeles

Step 3: After submitting a self-reported incident, you will be taken to the **Event Details page** for the incident you just created. You will be required to resolve this event by following the workflow described below.

This event will follow a similar workflow of an event that has been determined as “Not Normal” AND “Not Permitted.” During this workflow, you’ll need to investigate whether or not any breach exclusions apply and whether further breach response/notification is required.

Note: *Further instruction regarding the workflow for events determined as “Not Normal” AND “Not Permitted” is outlined in a following section of this guide, 7_Concept Overview: Event Resolution Workflows.*


Reporting
Logs
Upload
Partner Demo / 9876543210
Log Out

Event Details

Pending
PI-AA7VY0KI0OI

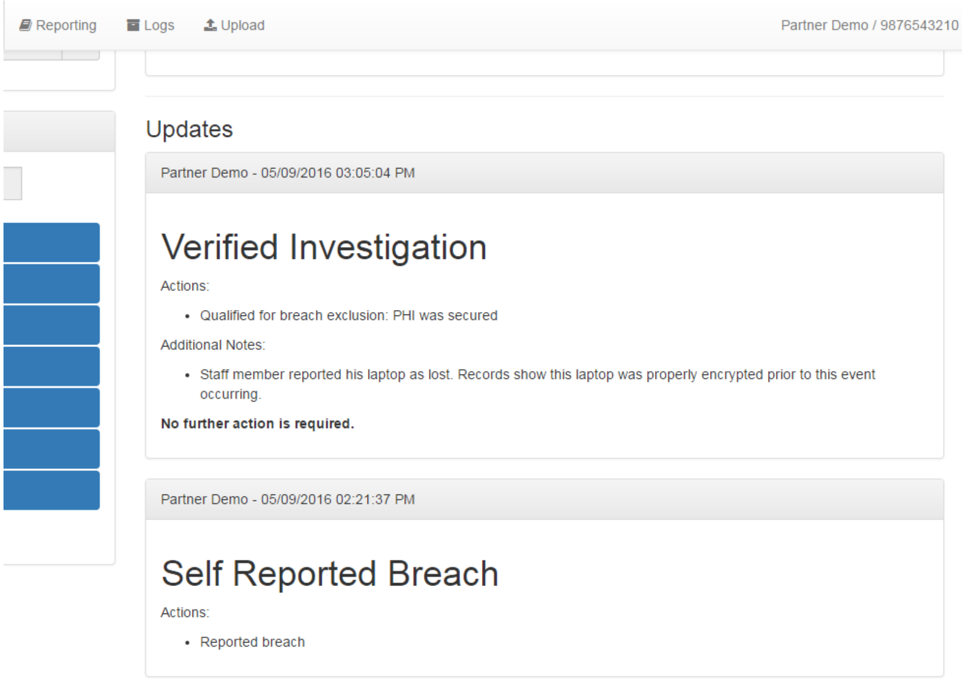
- Activity:Self Reported

Event Time	04/20/2016 12:00:00 AM
Discovery Time	04/25/2016 12:00:00 AM
User (1)	Ivan Sambilay
Patients (0)	
Affected Location	FusionCare Los Angeles
System	N/A
Log Records	View log records

Confirmation → Investigation → Remediation

Select all breach exclusions which apply to this incident:

Note: *Once you’ve completed the Event Resolution Workflow, event responses will be posted under the* ***Updates*** *section at the bottom of the* ***Event Details*** *page. It will also show the timestamp and name of the SPHER user who responded to the event.*



Updates

Partner Demo - 05/09/2016 03:05:04 PM

Verified Investigation

Actions:

- Qualified for breach exclusion: PHI was secured

Additional Notes:

- Staff member reported his laptop as lost. Records show this laptop was properly encrypted prior to this event occurring.

No further action is required.

Partner Demo - 05/09/2016 02:21:37 PM

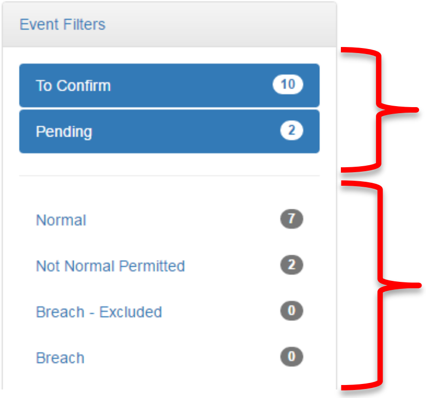
Self Reported Breach

Actions:

- Reported breach

6_Concept Overview: Event Statuses

Overview: Before you begin to investigate and resolve events detected by SPHER, it is important to understand the various status types that an event can hold. There are a total of 6 status types, 2 which represent new security events that require your immediate investigation and 4 which represent previously investigated and resolved events that are stored for your records as required by HIPAA. Users can filter by Event Status type using the Event Filters sidebar featured on the Events page.



Unresolved Statuses -
Events that require investigation or further action

Resolved Statuses -
Events that have been previously resolved (no further action required)

Unresolved Statuses - Events that require investigation or further action:

- **To Confirm** – This is a new detected event that requires immediate investigation.
- **Pending** – This is an event where upon after investigation, you determined that this event constituted user behavior that was both NOT NORMAL for the user(s) involved and NOT PERMITTED. However, the status is still considered pending because you have yet to resolve the event, i.e., investigate whether any Breach Exclusions apply or complete your Breach Response/Notification process.

Resolved Statuses - Events that have been previously resolved (no further action required):

- **Normal** – After investigation, you determined that this event constituted NORMAL user behavior for the user(s) involved.
- **Not Normal-Permitted** – After investigation, you determined that this event constituted user behavior that was NOT NORMAL for the user(s) involved, but in this instance was PERMITTED.
- **Breach-Excluded** – After investigation, you determined that this event constituted user behavior that was both NOT NORMAL for the user(s) involved and NOT PERMITTED. Upon further investigation, you've determined that specific breach exclusions DO apply.
- **Breach** – Similar to Breach-Excluded, you determined that this event constituted user behavior that was both NOT NORMAL and NOT PERMITTED. However, upon further investigation, you've determined that specific breach exclusions DO NOT apply. As a result, you have then completed your Breach Response/Notification process.

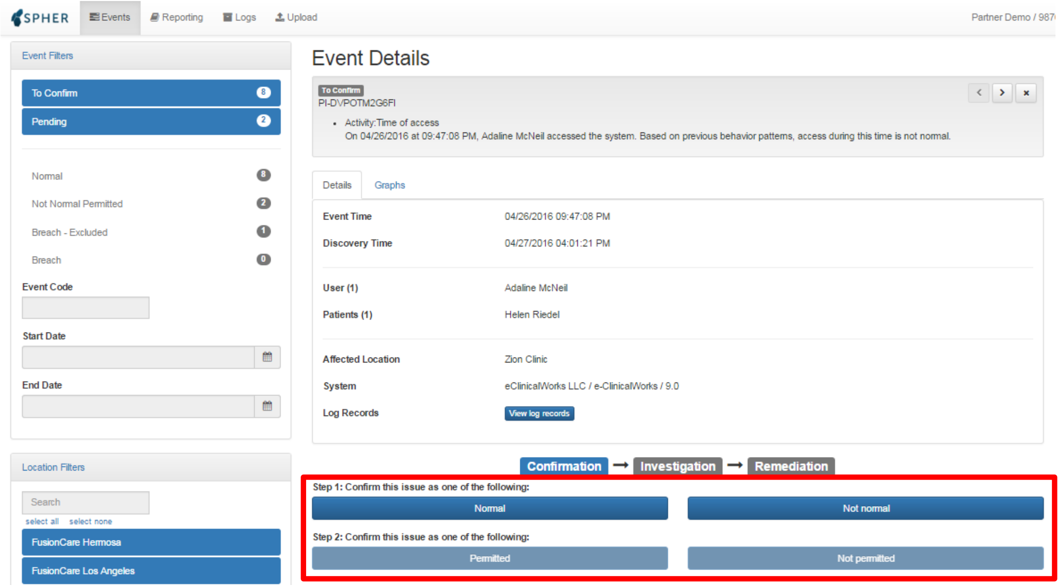
7_Concept Overview: Event Resolution Workflows

Overview: Now that you understand the status types that an event can hold, you can now begin to investigate and resolve events. Upon selecting an event to investigate, users can select how to respond to an event on the Events Details page.

Every detected event with a status of "To Confirm" can be responded to in one of 3 ways:

1. Normal
2. Not Normal AND Permitted
3. Not Normal AND Not Permitted

You will find a section displaying these response options below the event details.



Event Details

To Confirm
PI-DVPOTM2G6FI

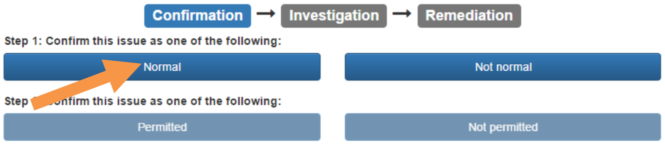
- Activity:Time of access
  On 04/26/2016 at 09:47:08 PM, Adaline McNeil accessed the system. Based on previous behavior patterns, access during this time is not normal.

Event Time	04/26/2016 09:47:08 PM
Discovery Time	04/27/2016 04:01:21 PM
User (1)	Adaline McNeil
Patients (1)	Helen Riedel
Affected Location	Zion Clinic
System	eClinicalWorks LLC / e-ClinicalWorks / 9.0
Log Records	View log records

Step 1: Confirm this issue as one of the following:

Step 2: Confirm this issue as one of the following:

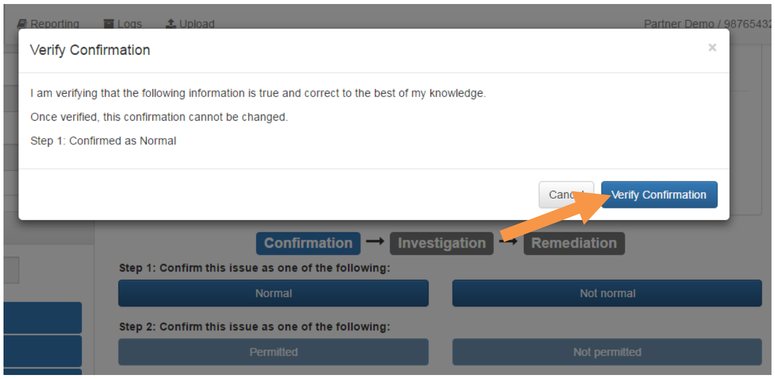
- **Responding as "Normal"**



Step 1: Confirm this issue as one of the following:

Step onfirm this issue as one of the following:

  - By responding "Normal," you are defining the user's activity in question as normal. A response of "Normal" informs SPHER to learn the event as normal behavior for the user involved. Should SPHER detect similar activity from this user in the future, SPHER will no longer alert you.
  - You will be prompted to verify your response. As this event represents normal user behavior, no further documentation is required.



Verify Confirmation

I am verifying that the following information is true and correct to the best of my knowledge.

Once verified, this confirmation cannot be changed.

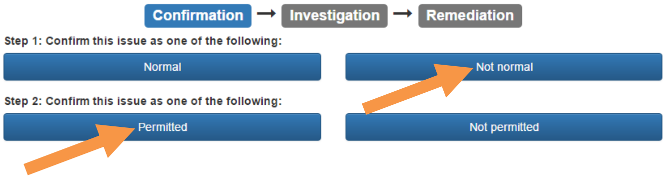
Step 1: Confirmed as Normal

Step 1: Confirm this issue as one of the following:

Step 2: Confirm this issue as one of the following:

- Once verified, this event will change to a **resolved status of NORMAL**.

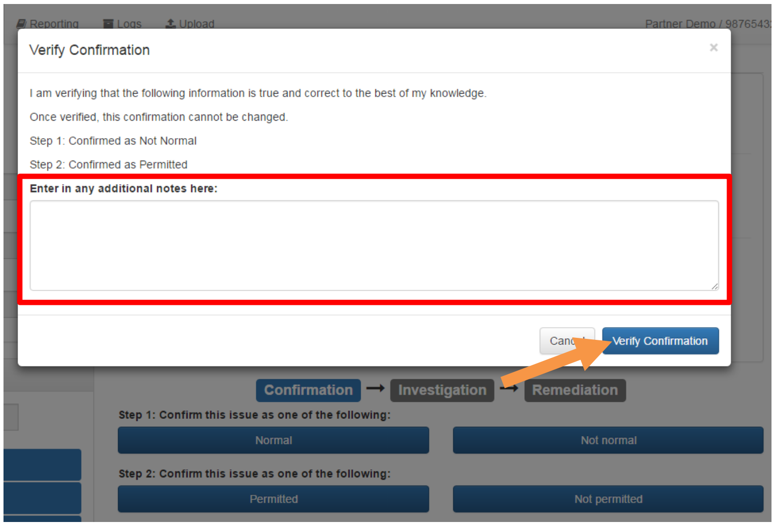
- **Responding as “Not Normal” and “Permitted”**



Step 1: Confirm this issue as one of the following:

Step 2: Confirm this issue as one of the following:

  - By responding “Not Normal,” you are defining the user’s activity in question as not normal. As this activity is not normal, SPHER will not learn this activity as part of the user’s profile and will continue to alert you should SPHER detect similar activity from this user in the future.
  - Since you are also responding “Permitted,” you will be prompted verify your response. As this event represents behavior that is not normal yet permitted, it is recommended that you document a brief explanation of why the event is considered permitted.



Verify Confirmation

I am verifying that the following information is true and correct to the best of my knowledge.

Once verified, this confirmation cannot be changed.

Step 1: Confirmed as Not Normal

Step 2: Confirmed as Permitted

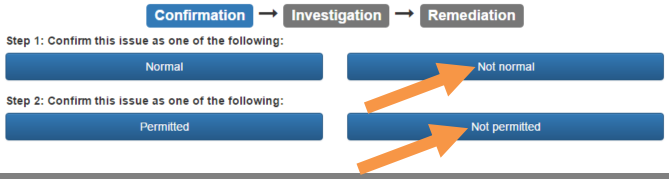
Enter in any additional notes here:

Step 1: Confirm this issue as one of the following:

Step 2: Confirm this issue as one of the following:

  - Once verified, this event will change to a **resolved status of NOT NORMAL-PERMITTED**.

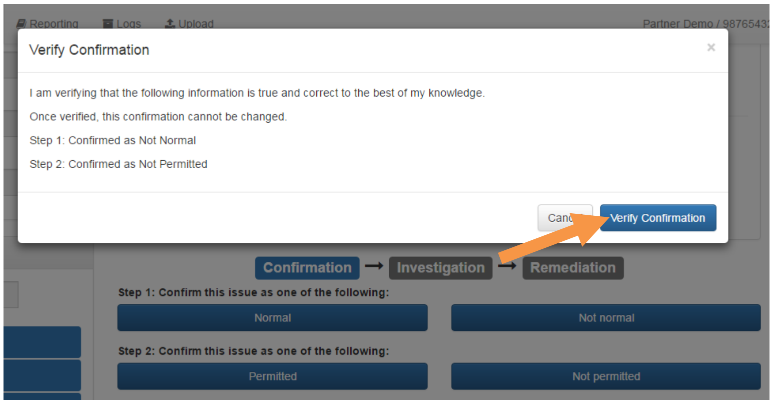
- **Responding as “Not Normal” and “Not Permitted”**
  - There are two possible workflows that can result from a response of “Not Normal” and “Not Permitted,” which will be described in further detail in this section.



Step 1: Confirm this issue as one of the following:

Step 2: Confirm this issue as one of the following:

- As mentioned previously, a response of "Not Normal" will result in SPHER not learning this activity as part of the user's profile.
- By responding "Not Permitted," you are defining the detected event as a possible breach as defined in §164.402 of the HIPAA Omnibus Final Rule. As a result from your response, you'll be prompted to investigate whether any Breach Exclusions apply to this event.



Verify Confirmation

I am verifying that the following information is true and correct to the best of my knowledge.

Once verified, this confirmation cannot be changed.

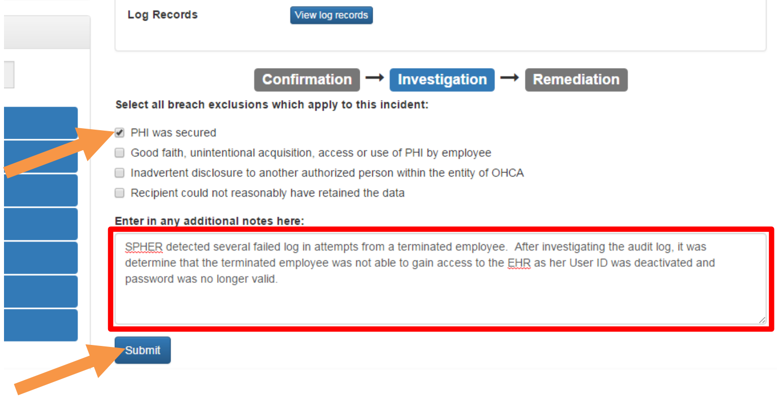
Step 1: Confirmed as Not Normal

Step 2: Confirmed as Not Permitted

Step 1: Confirm this issue as one of the following:

Step 2: Confirm this issue as one of the following:

- As a result of your further investigation, select any Breach Exclusions that apply to this event which exclude it from being a breach and document any additional notes in the text box below and click Submit. If you determine that exclusions do not apply and this event is a breach, do not select any exclusions and document any additional notes below and click Submit.



Log Records

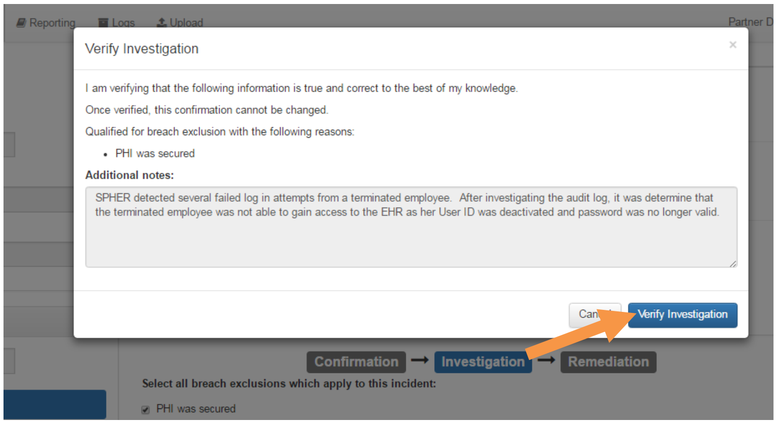
Select all breach exclusions which apply to this incident:

☑ PHI was secured
☐ Good faith, unintentional acquisition, access or use of PHI by employee
☐ Inadvertent disclosure to another authorized person within the entity of OHCA
☐ Recipient could not reasonably have retained the data

Enter in any additional notes here:

SPHER detected several failed log in attempts from a terminated employee. After investigating the audit log, it was determine that the terminated employee was not able to gain access to the EHR as her User ID was deactivated and password was no longer valid.

- If you selected any Breach Exclusions during the previous step, you will be prompted to review and verify your response. Once verified, this event will change to a **resolved status of BREACH-EXCLUDED**.



Verify Investigation

I am verifying that the following information is true and correct to the best of my knowledge.

Once verified, this confirmation cannot be changed.

Qualified for breach exclusion with the following reasons:

- PHI was secured

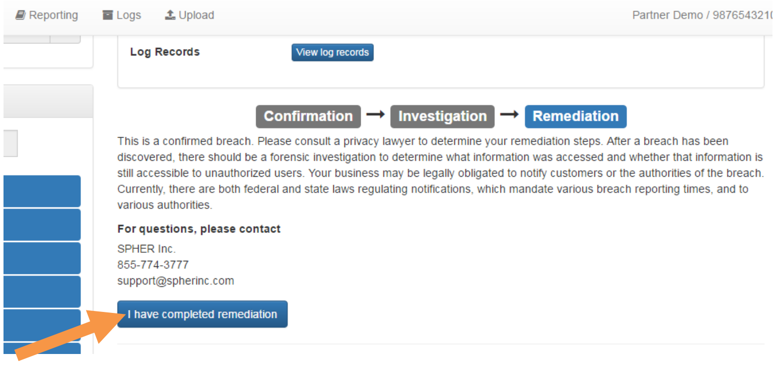
Additional notes:

SPHER detected several failed log in attempts from a terminated employee. After investigating the audit log, it was determine that the terminated employee was not able to gain access to the EHR as her User ID was deactivated and password was no longer valid.

Select all breach exclusions which apply to this incident:

☑ PHI was secured

- If you did not select any Breach Exclusions during the previous step, you are confirming that this event is a breach. As such, you must remediate the breach undergo your Breach Response/Notification process. Once remediation is complete click the "I have completed remediation button."


Reporting
Logs
Upload
Partner Demo / 987654321(

Log Records View log records

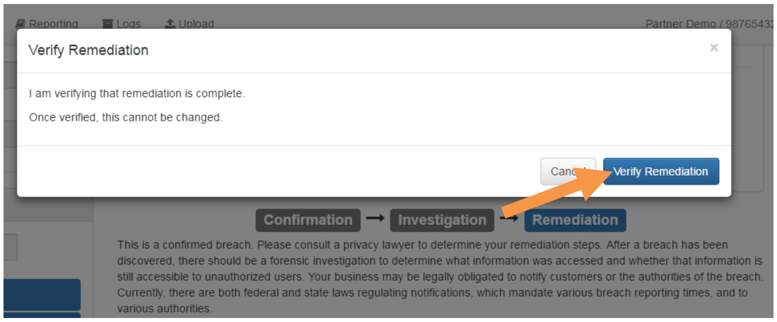
Confirmation → Investigation → Remediation

This is a confirmed breach. Please consult a privacy lawyer to determine your remediation steps. After a breach has been discovered, there should be a forensic investigation to determine what information was accessed and whether that information is still accessible to unauthorized users. Your business may be legally obligated to notify customers or the authorities of the breach. Currently, there are both federal and state laws regulating notifications, which mandate various breach reporting times, and to various authorities.

For questions, please contact

SPHER Inc.
855-774-3777
support@spherinc.com

- You will be prompted to verify your response.



Verify Remediation

I am verifying that remediation is complete.

Once verified, this cannot be changed.

This is a confirmed breach. Please consult a privacy lawyer to determine your remediation steps. After a breach has been discovered, there should be a forensic investigation to determine what information was accessed and whether that information is still accessible to unauthorized users. Your business may be legally obligated to notify customers or the authorities of the breach. Currently, there are both federal and state laws regulating notifications, which mandate various breach reporting times, and to various authorities.

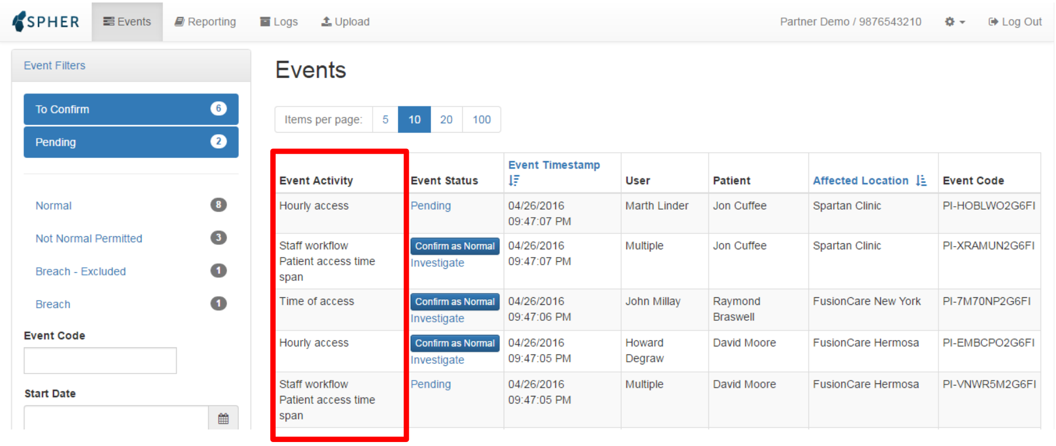
- Once verified, this event will change to a **resolved status of BREACH**.

8_Concept Overview: Activity Detectors

Overview: SPHER detects irregular user activities through the use of various algorithms, referred to in SPHER as Activity Detectors. These Activity Detectors analyze different components of a user's behavior in order to identify normal baselines of activity and create unique user profiles for each individual user or group of users. Each Activity Detector bases its baselines on a 60 day trailing window of previous user activity.

The types of **Activity Detectors** are displayed for each event on the **Events Page** in the **Events Table** and also on the **Event Details page**. This information is vital during the investigation process for any event. The definitions and examples for the Activity Detectors are outlined in this section.

Events Page (Events Table)

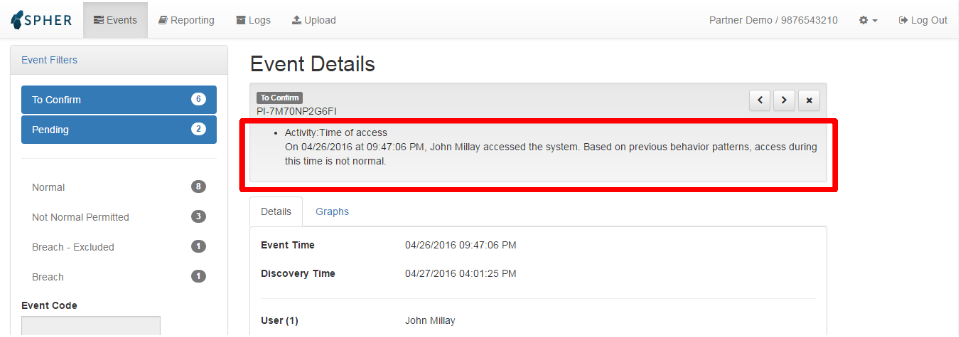


Events

Items per page: 5 10 20 100

Event Activity	Event Status	Event Timestamp	User	Patient	Affected Location	Event Code
Hourly access	Pending	04/26/2016 09:47:07 PM	Marth Linder	Jon Cuffee	Spartan Clinic	PI-HOBLWO2G6FI
Staff workflow Patient access time span	Confirm as Normal Investigate	04/26/2016 09:47:07 PM	Multiple	Jon Cuffee	Spartan Clinic	PI-XRAMUN2G6FI
Time of access	Confirm as Normal Investigate	04/26/2016 09:47:06 PM	John Millay	Raymond Braswell	FusionCare New York	PI-7M70NP2G6FI
Hourly access	Confirm as Normal Investigate	04/26/2016 09:47:05 PM	Howard Degraw	David Moore	FusionCare Hermosa	PI-EMBCPO2G6FI
Staff workflow Patient access time span	Pending	04/26/2016 09:47:05 PM	Multiple	David Moore	FusionCare Hermosa	PI-VNWR5M2G6FI

Event Details Page



Event Details

To Confirm
PI-7M70NP2G6FI

- Activity:Time of access
  On 04/26/2016 at 09:47:06 PM, John Millay accessed the system. Based on previous behavior patterns, access during this time is not normal.

Event Time	04/26/2016 09:47:06 PM
Discovery Time	04/27/2016 04:01:25 PM
User (1)	John Millay

Self-examination – This detector will alert you when a user is accessing his or her own patient record.

For example: A user modifies her own patient record.

Last name matching – This detector will alert you when a user is accessing a patient that has the same last name.

For example: A user named Ivan Kan is accessing the record of patient named Andrew Kan.

Time of access – This detector will alert you when a user is accessing the system outside of his or her normal time of access.

> For example: A user historically has accessed the system consistently between 9:00 AM to 5:00 PM. This user then recently accesses the system at 11:49 PM to 12:27 AM which is detected by SPHER.

Hourly access – This detector will alert you when a user's amount of activity on the system per hour is outside of his or her normal range of activity.

> For example: A particular user has a normal hourly activity range of use of 50 to 75 user activities per hour. These activities include checking in a patient, entering notes on a patient, and printing medical records. SPHER detected an event where this user used the system to print more medical records than she normally does which resulted in 300 user activities in an hour.

Patient access time span – This detector will alert you when the length of time a patient's record is being accessed is longer than normal.

> For example: The maximum time span for which a patient's record is accessed for this particular medical group is 57 minutes which includes check in to check out. Several users accessed a particular patient's record from 9:31 AM to 5:52 PM. The time span that this patient's record has been accessed is 8 hours 21 minutes which is longer than usual.

Staff workflow – This detector will alert you when the order of users accessing a patient record does not match a previously known sequence.

> For example: A common staff workflow on patient access for this particular medical group is Eunice, Amy, Andrew, Dr. Kan, then finally back to Eunice (all users within the same OBGYN department). However, SPHER detected a random sequence of users accessing a patient record which included Amy and Eunice but also included April, Kristen, and May (users from different departments). As this detector has never seen this particular sequence of users accessing a single patient record, SPHER has alerted you.

Role workflow – Similar to Staff Workflow, this detector will alert you when the roles of users accessing a patient record do not match a previously known sequence.

> For example: Similar to example above for "Staff workflow," the staff sequence of Eunice, Amy, Andrew, Dr. Kan, then back to Eunice have roles defined within the EHR as Front Desk, Medical Assistant, Nurse, Physician, then back to Front desk. This is a common role workflow representing a patient being handled by users from check-in to check-out. However, SPHER detected an event where the sequence of roles was Medical Assistant (Amy), Front Desk (Eunice), Biller (April), Medical Assistant (Kristen), Nurse (May). As this detector has never seen this particular sequence of user roles accessing a single patient record, SPHER has alerted you.

9_Guide to Investigating and Resolving Events

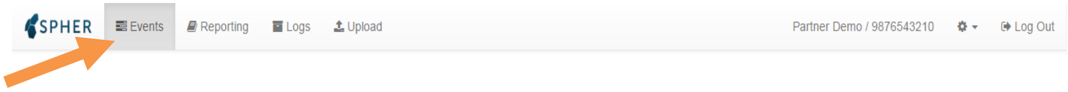
Overview: This Quick Start Guide to Resolving Events will outline the complete workflow of how SPHER users can easily investigate and resolve events in SPHER. Throughout this section, should you require further instruction on the various functions of SPHER outside of investigating and resolving events, references to other sections of this guide will be provided when applicable.

If you have received an **Alert** via an **Event Notification email** notifying you of events that need to be reviewed, you will need to log in to SPHER in order to investigate and resolve them. To investigate and resolve the events, follow the workflow instructions below:

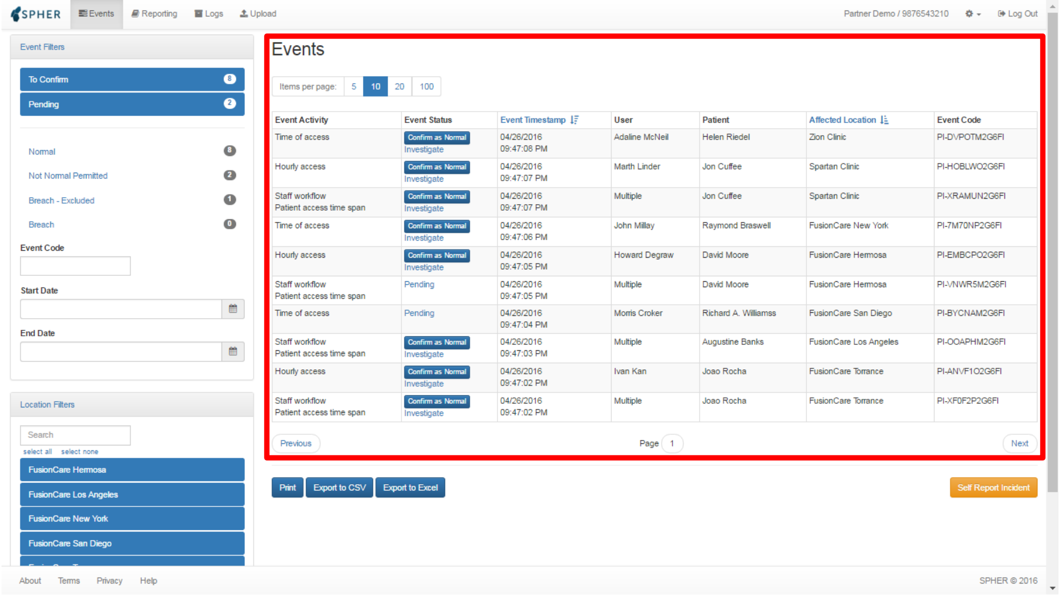
Step 1: Go to **dashboard.amsspher.com** and log in to your SPHER account. Alternatively, if you are currently viewing the **Event Notification email**, click the **SPHER Portal** link found within the Event Notification email and it will take you to the log in page.

Step 2: To navigate to the **Events** page click the **Events tab** at the top of your screen.

Note: *For SPHER users with permissions to view the Events page, this page will open by default upon log in.*



Step 3: Locate the list of events that need to be resolved in the **Events table** on the right of the Event and Location Filters sidebar.



Events

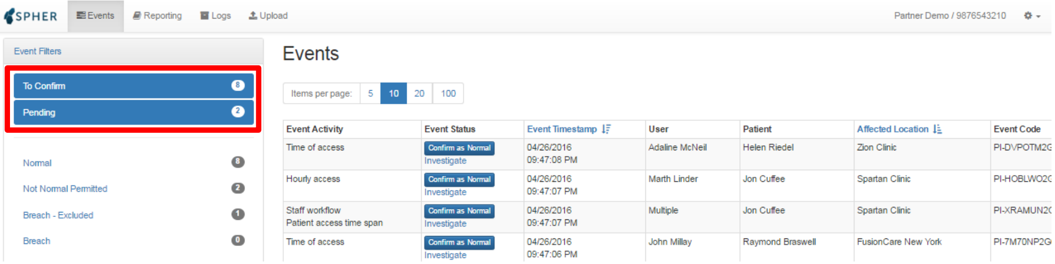
Items per page: 5 10 20 100

Event Activity	Event Status	Event Timestamp	User	Patient	Affected Location	Event Code
Time of access	Confirm as Normal Investigate	04/26/2016 09:47:08 PM	Adaline McNeil	Helen Riedel	Zion Clinic	PI-DVPOTM2G6FI
Hourly access	Confirm as Normal Investigate	04/26/2016 09:47:07 PM	Marth Linder	Jon Cuffee	Spartan Clinic	PI-HOBLWO2G6FI
Staff workflow Patient access time span	Confirm as Normal Investigate	04/26/2016 09:47:07 PM	Multiple	Jon Cuffee	Spartan Clinic	PI-XRAMUN2G6FI
Time of access	Confirm as Normal Investigate	04/26/2016 09:47:06 PM	John Millay	Raymond Braswell	FusionCare New York	PI-7M70NP2G6FI
Hourly access	Confirm as Normal Investigate	04/26/2016 09:47:05 PM	Howard Degraw	David Moore	FusionCare Hermosa	PI-EMBCPO2G6FI
Staff workflow Patient access time span	Pending	04/26/2016 09:47:05 PM	Multiple	David Moore	FusionCare Hermosa	PI-VNWR5M2G6FI
Time of access	Pending	04/26/2016 09:47:04 PM	Morris Croker	Richard A. Williamss	FusionCare San Diego	PI-BYCNAM2G6FI
Staff workflow Patient access time span	Confirm as Normal Investigate	04/26/2016 09:47:03 PM	Multiple	Augustine Banks	FusionCare Los Angeles	PI-OOAPHM2G6FI
Hourly access	Confirm as Normal Investigate	04/26/2016 09:47:02 PM	Ivan Kan	Joao Rocha	FusionCare Torrance	PI-ANVF1O2G6FI
Staff workflow Patient access time span	Confirm as Normal Investigate	04/26/2016 09:47:02 PM	Multiple	Joao Rocha	FusionCare Torrance	PI-XF0F2P2G6FI

Previous Page 1 Next

Print Export to CSV Export to Excel Self Report Incident

Note: *Upon logging in, you will notice that ALL events that have yet to be investigated or resolved and require your immediate attention, i.e., "To Confirm" and "Pending" status, are selected by default in the* ***Event Filters sidebar****. Events that you have previously resolved in the past and no longer require your attention, i.e., "Normal," "Not Normal-Permitted," "Breach-Excluded," and "Breach" status, are deselected by default. For more information on previously resolved events, see the following section of this guide, 6_Concept Overview: Event Statuses.*



Event Filters

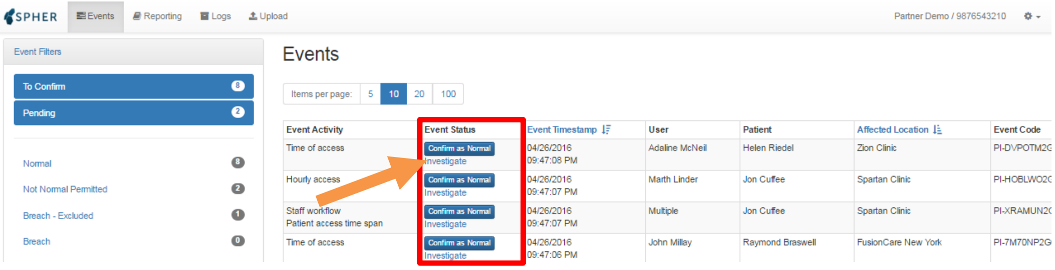
- To Confirm 8
- Pending 2
- Normal 8
- Not Normal Permitted 2
- Breach - Excluded 1
- Breach 0

Events

Items per page: 5 10 20 100

Event Activity	Event Status	Event Timestamp	User	Patient	Affected Location	Event Code
Time of access	Confirm as Normal Investigate	04/26/2016 09:47:08 PM	Adaline McNeil	Helen Riedel	Zion Clinic	PI-DVPOTM2G
Hourly access	Confirm as Normal Investigate	04/26/2016 09:47:07 PM	Marth Linder	Jon Cuffee	Spartan Clinic	PI-HOBLWO2C
Staff workflow Patient access time span	Confirm as Normal Investigate	04/26/2016 09:47:07 PM	Multiple	Jon Cuffee	Spartan Clinic	PI-XRAMUN2C
Time of access	Confirm as Normal Investigate	04/26/2016 09:47:06 PM	John Millay	Raymond Braswell	FusionCare New York	PI-7M70NP2G

Step 4: Click the **"Investigate" link** of the event that you would like to investigate in the Event Status column of the Events table. This will take you to the **Event Details page** for that particular event.



Event Filters

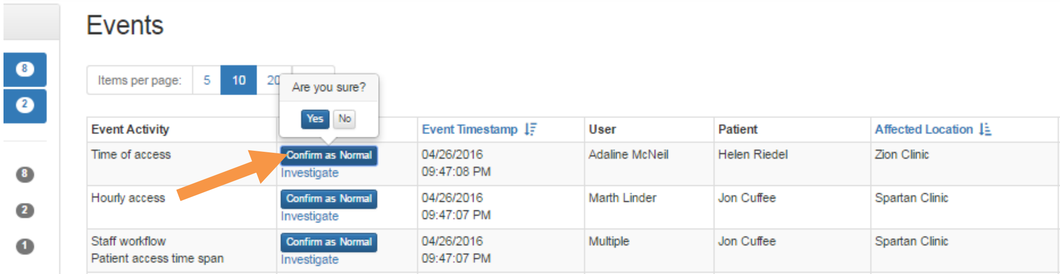
- To Confirm 8
- Pending 2
- Normal 8
- Not Normal Permitted 2
- Breach - Excluded 1
- Breach 0

Events

Items per page: 5 10 20 100

Event Activity	Event Status	Event Timestamp	User	Patient	Affected Location	Event Code
Time of access	Confirm as Normal Investigate	04/26/2016 09:47:08 PM	Adaline McNeil	Helen Riedel	Zion Clinic	PI-DVPOTM2G
Hourly access	Confirm as Normal Investigate	04/26/2016 09:47:07 PM	Marth Linder	Jon Cuffee	Spartan Clinic	PI-HOBLWO2C
Staff workflow Patient access time span	Confirm as Normal Investigate	04/26/2016 09:47:07 PM	Multiple	Jon Cuffee	Spartan Clinic	PI-XRAMUN2C
Time of access	Confirm as Normal Investigate	04/26/2016 09:47:06 PM	John Millay	Raymond Braswell	FusionCare New York	PI-7M70NP2G

Note: *Alternatively, if you find that this event does not require additional investigation and want to quickly respond to this event with a resolved status of "Normal," click the **"Confirm as Normal" button**.*



Events

Items per page: 5 10 20

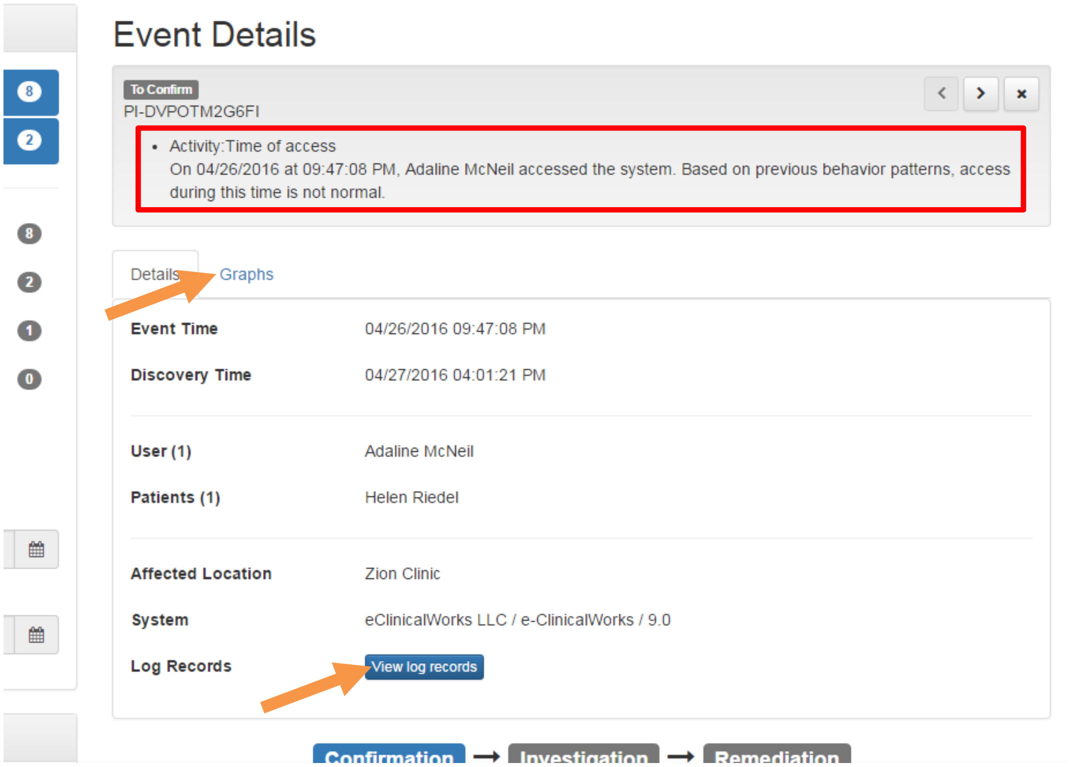
Are you sure?

Yes No

Event Activity		Event Timestamp	User	Patient	Affected Location
Time of access	Confirm as Normal Investigate	04/26/2016 09:47:08 PM	Adaline McNeil	Helen Riedel	Zion Clinic
Hourly access	Confirm as Normal Investigate	04/26/2016 09:47:07 PM	Marth Linder	Jon Cuffee	Spartan Clinic
Staff workflow Patient access time span	Confirm as Normal Investigate	04/26/2016 09:47:07 PM	Multiple	Jon Cuffee	Spartan Clinic

Step 4: The **Event Details page** will display the details of the event needed for you to investigate. A description of the type of Activity that was detected by SPHER is provided at the top of the page.

You can investigate further by viewing the **Event Graph** or **Viewing the Log Records**.



Event Details

To Confirm

PI-DVPOTM2G6FI

- Activity:Time of access
  On 04/26/2016 at 09:47:08 PM, Adaline McNeil accessed the system. Based on previous behavior patterns, access during this time is not normal.

Event Time 04/26/2016 09:47:08 PM

Discovery Time 04/27/2016 04:01:21 PM

User (1) Adaline McNeil

Patients (1) Helen Riedel

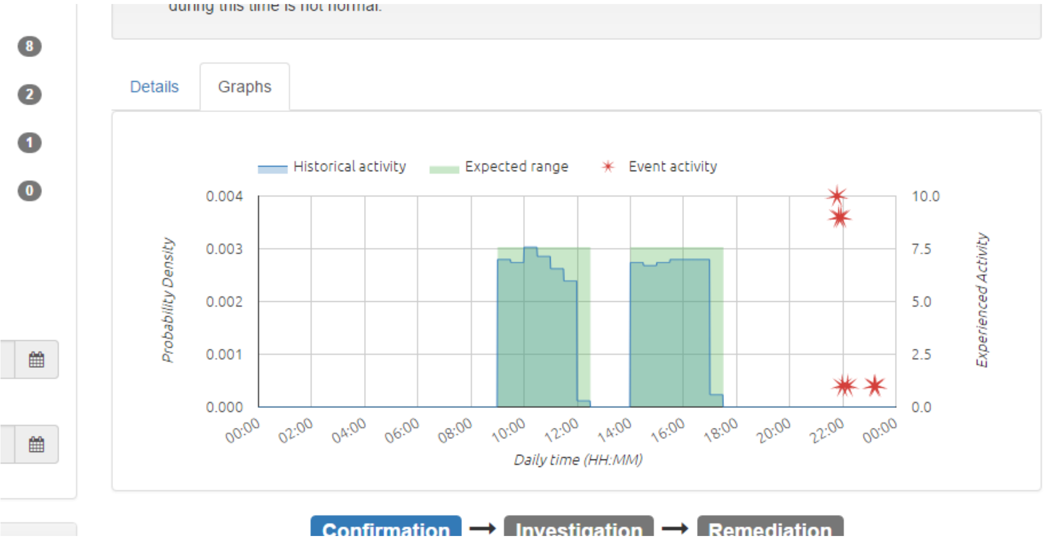
Affected Location Zion Clinic

System eClinicalWorks LLC / e-ClinicalWorks / 9.0

Log Records View log records

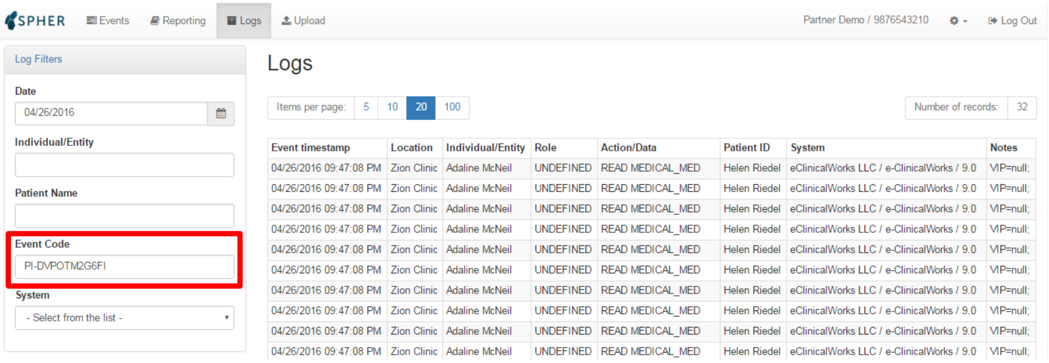
Event Graph: Clicking the Graph tab will display a graph specific to the type of activity that was detected. The graph will display 3 variables:

- Expected Range – This is the range SPHER has learned as normal behavior for this user.
- Historical Activity – This is the user's activity that fell within the range SPHER expects as normal.
- Event Activity – This is the user's activity that fell outside the range SPHER expects as normal. Each red asterisk represents a record within the audit log file.



during this time is not normal.

View Log Records: Clicking the **View Log Records button** automatically takes you to the **Logs page** that displays the log records for this specific event. Notice that the code for the event has been auto-filled. This is helpful when reviewing the exact individual actions performed by the user(s) involved in the order which they occurred.



Date: 04/26/2016

Individual/Entity:

Patient Name:

Event Code: PI-DVPOTM2G6FI

System: - Select from the list -

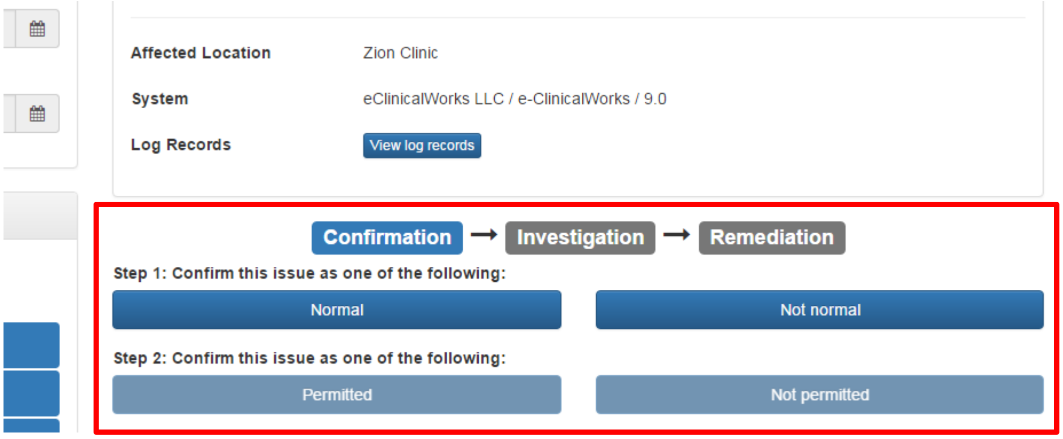
Logs

Items per page: 5 | 10 | 20 | 100

Number of records: 32

Event timestamp	Location	Individual/Entity	Role	Action/Data	Patient ID	System	Notes
04/26/2016 09:47:08 PM	Zion Clinic	Adaline McNeil	UNDEFINED	READ MEDICAL_MED	Helen Riedel	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:08 PM	Zion Clinic	Adaline McNeil	UNDEFINED	READ MEDICAL_MED	Helen Riedel	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:08 PM	Zion Clinic	Adaline McNeil	UNDEFINED	READ MEDICAL_MED	Helen Riedel	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:08 PM	Zion Clinic	Adaline McNeil	UNDEFINED	READ MEDICAL_MED	Helen Riedel	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:08 PM	Zion Clinic	Adaline McNeil	UNDEFINED	READ MEDICAL_MED	Helen Riedel	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:08 PM	Zion Clinic	Adaline McNeil	UNDEFINED	READ MEDICAL_MED	Helen Riedel	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:08 PM	Zion Clinic	Adaline McNeil	UNDEFINED	READ MEDICAL_MED	Helen Riedel	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:08 PM	Zion Clinic	Adaline McNeil	UNDEFINED	READ MEDICAL_MED	Helen Riedel	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:08 PM	Zion Clinic	Adaline McNeil	UNDEFINED	READ MEDICAL_MED	Helen Riedel	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:08 PM	Zion Clinic	Adaline McNeil	UNDEFINED	READ MEDICAL_MED	Helen Riedel	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;

Step 5: Once you've completed your investigation for this event, scroll down to the bottom of the page to see the **Event Resolution Workflow**. To respond to this event, click on the button that corresponds to the confirmation question being answered.



Affected Location: Zion Clinic

System: eClinicalWorks LLC / e-ClinicalWorks / 9.0

Log Records: View log records

Step 1: Confirm this issue as one of the following:

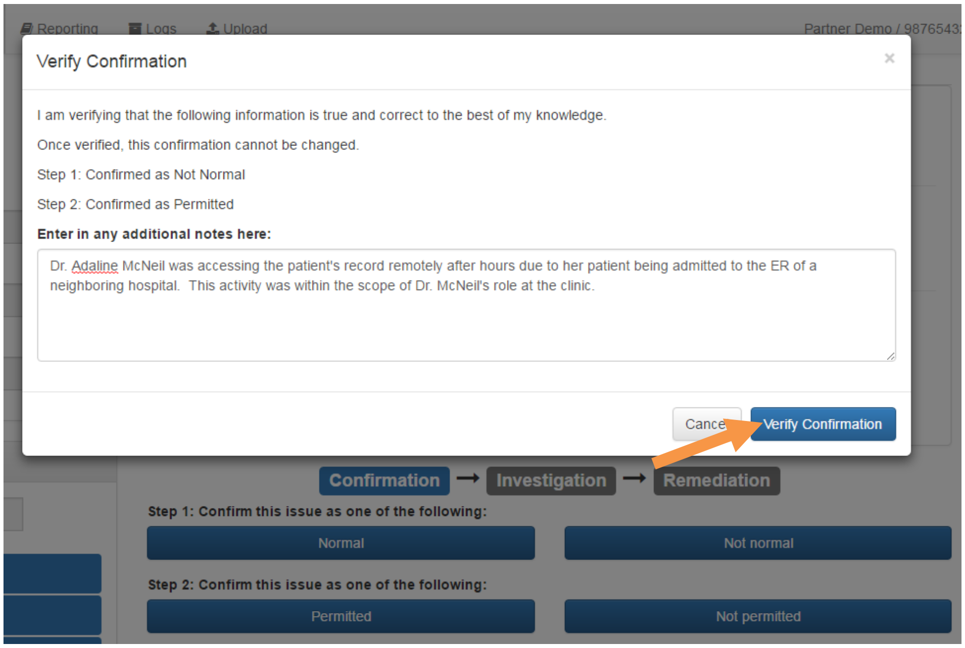
Step 2: Confirm this issue as one of the following:

***Note:** The next steps of the **Event Resolution Workflow** will depend on your response. For example, incidents that are determined to be **Normal** will not have Investigation and Remediation tasks nor require additional notes. Similarly, incidents that determined to be **Normal and Permitted** will not have Investigations and Remediation tasks but will require additional notes.*

*If your **Confirmation** response of **Not Normal and Not Permitted** takes you to **Investigation**, if at least one of the breach exclusions applies to the event, then the event is not considered a breach, and no remediation step is required, otherwise it will take you to **Remediation**. You may enter additional notes regarding this event on the text box before clicking **Submit**.*

For more information on Event Resolution Workflow, see the previous section of this guide, 7_Concept Overview: Event Resolution Workflows.

Step 6: For all Event Resolutions Workflows, a popup window will display prompting you to verify your response. Depending on your response, additional notes to summarize your findings may be required. Review your response carefully as this confirmation cannot be reversed, then click the **Verify button**.



Verify Confirmation

I am verifying that the following information is true and correct to the best of my knowledge.

Once verified, this confirmation cannot be changed.

Step 1: Confirmed as Not Normal

Step 2: Confirmed as Permitted

Enter in any additional notes here:

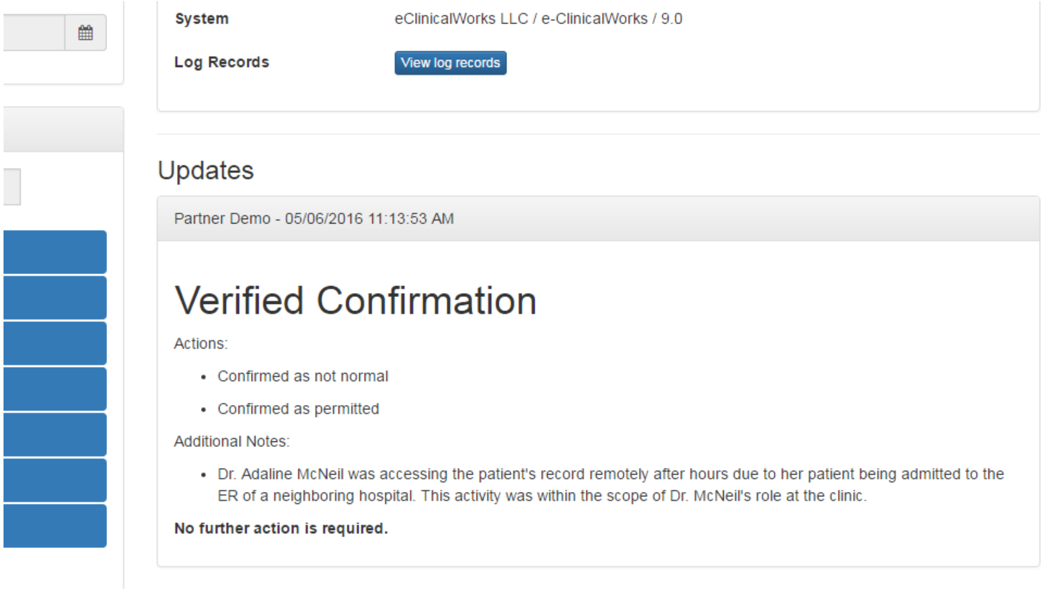
Dr. Adaline McNeil was accessing the patient's record remotely after hours due to her patient being admitted to the ER of a neighboring hospital. This activity was within the scope of Dr. McNeil's role at the clinic.

Confirmation → Investigation → Remediation

Step 1: Confirm this issue as one of the following:

Step 2: Confirm this issue as one of the following:

Note: *Once you've completed the Event Resolution Workflow, event responses will be posted under the* ***Updates*** *section at the bottom of the* ***Event Details page****. It will also show the timestamp and name of the SPHER user who responded to the event.*



System	eClinicalWorks LLC / e-ClinicalWorks / 9.0
Log Records	View log records

Updates

Partner Demo - 05/06/2016 11:13:53 AM

Verified Confirmation

Actions:

- Confirmed as not normal
- Confirmed as permitted

Additional Notes:

- Dr. Adaline McNeil was accessing the patient's record remotely after hours due to her patient being admitted to the ER of a neighboring hospital. This activity was within the scope of Dr. McNeil's role at the clinic.

No further action is required.

10_Logs Page

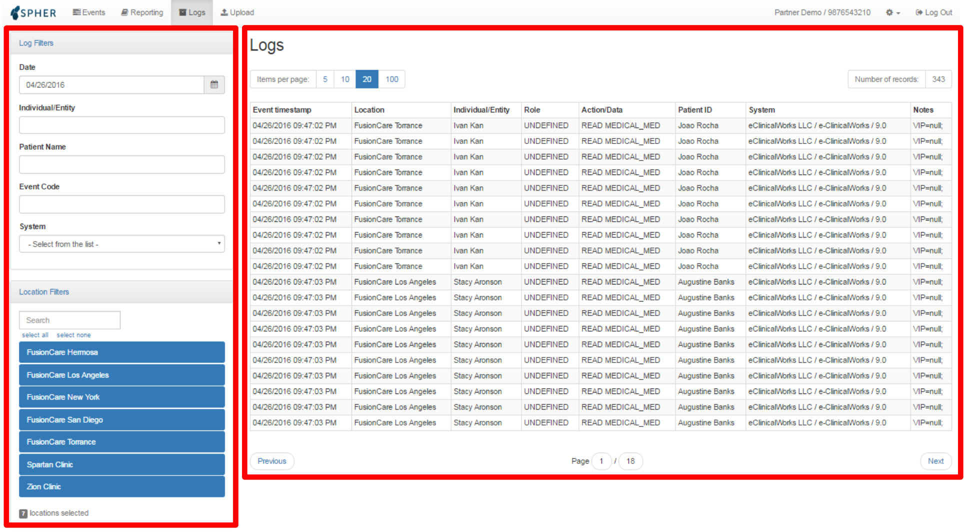
Overview: SPHER allows for users to view the Audit Logs that have been previously uploaded and analyzed by SPHER. Various filters are found on the Logs page that allow a user to sort by date, user, patient, event code, EHR/system (for organizations with multiple systems), and location (for organizations with multiple locations and/or departments).

Common uses of the Logs Page include:

- Responding to a patient's inquiry to investigate whether his or her data has been used or disclosed by employees in an inappropriate manner (a SPHER user can filter user activity against a specific patient)
- Investigating a specific user's activity that is in the process of being terminated or suspected of malfeasance (A SPHER user can filter user activity against a specific user)

This section of the guide will provide an overview of the following features and functions of the Logs page:

- Logs Table
- Log Filters and Location Filters



Log Filters

Date: 04/26/2016

Individual/Entity:

Patient Name:

Event Code:

System: - Select from the list -

Location Filters

Search

select all   select none

- FusionCare Hermosa
- FusionCare Los Angeles
- FusionCare New York
- FusionCare San Diego
- FusionCare Torrance
- Spartan Clinic
- Zion Clinic

7 locations selected

Logs

Items per page: 5 10 20 100

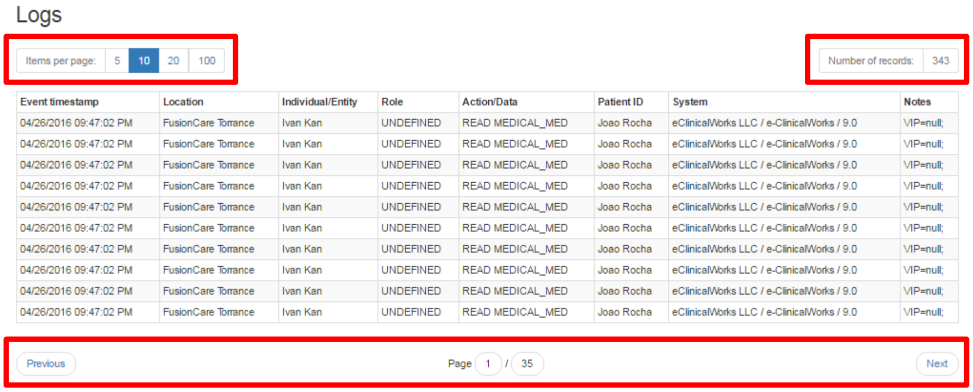
Number of records: 343

Event timestamp	Location	Individual/Entity	Role	Action/Data	Patient ID	System	Notes
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:03 PM	FusionCare Los Angeles	Stacy Aronson	UNDEFINED	READ MEDICAL_MED	Augustine Banks	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:03 PM	FusionCare Los Angeles	Stacy Aronson	UNDEFINED	READ MEDICAL_MED	Augustine Banks	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:03 PM	FusionCare Los Angeles	Stacy Aronson	UNDEFINED	READ MEDICAL_MED	Augustine Banks	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:03 PM	FusionCare Los Angeles	Stacy Aronson	UNDEFINED	READ MEDICAL_MED	Augustine Banks	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:03 PM	FusionCare Los Angeles	Stacy Aronson	UNDEFINED	READ MEDICAL_MED	Augustine Banks	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:03 PM	FusionCare Los Angeles	Stacy Aronson	UNDEFINED	READ MEDICAL_MED	Augustine Banks	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:03 PM	FusionCare Los Angeles	Stacy Aronson	UNDEFINED	READ MEDICAL_MED	Augustine Banks	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:03 PM	FusionCare Los Angeles	Stacy Aronson	UNDEFINED	READ MEDICAL_MED	Augustine Banks	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:03 PM	FusionCare Los Angeles	Stacy Aronson	UNDEFINED	READ MEDICAL_MED	Augustine Banks	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:03 PM	FusionCare Los Angeles	Stacy Aronson	UNDEFINED	READ MEDICAL_MED	Augustine Banks	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;

10.1_Logs Table

Overview: The Logs Table shows you a list of all the activity conducted by users on the EHR/systems that has been previously uploaded and analyzed by SPHER. The logs are useful in understanding what EHR users have done while logged into a specific system. Within the logs table, user activity is displayed in chronological order.

Navigating the Logs table can be done in a number of ways. At the upper-left corner of the Logs table, you can select the number of events per page you would like to view. At the upper-right hand corner, there is a counter that displays the number of records, i.e., lines of captured user activity. Should any log filters or location filters be selected, this number will change to reflect your selection. At the bottom of the logs table you can use the buttons to skip pages; the page number can also be found at the bottom.



Event timestamp	Location	Individual/Entity	Role	Action/Data	Patient ID	System	Notes
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;
04/26/2016 09:47:02 PM	FusionCare Torrance	Ivan Kan	UNDEFINED	READ MEDICAL_MED	Joao Rocha	eClinicalWorks LLC / e-ClinicalWorks / 9.0	VIP=null;

There are 8 columns within the logs table that define the information contained within the audit logs:

- Event timestamp
- Location
- Individual/Entity
- Role
- Action/Data (e.g., Read, Modify, or Delete)
- Patient ID
- System
- More (displays any custom fields found within the Audit Log, e.g., “VIP = Yes/No”)

***Note:** Custom fields found within the Audit Log vary from system to system.*

10.2_Log Filters and Location Filters

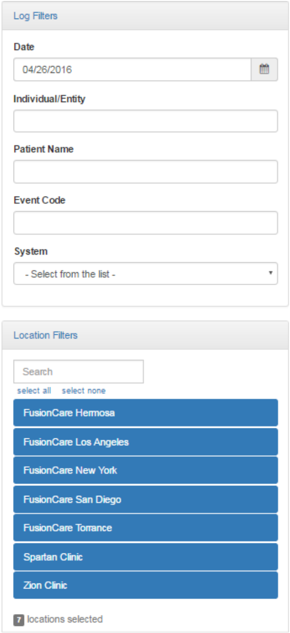
Overview: SPHER users can apply various log and location filters.

The Log Filters available to a user are as follows:

- Date
- Individual/Entity
- Patient Name
- Event Code
- System

The Location filters allow a user to sort by specific locations. Quick select options exist should a user want to select all or select none or search for the name of an individual location.

Note: *Locations can represent separate offices of a medical group or separate departments within a hospital system.*



Log Filters

Date

04/26/2016

Individual/Entity

Patient Name

Event Code

System

- Select from the list -

Location Filters

FusionCare Hermosa
FusionCare Los Angeles
FusionCare New York
FusionCare San Diego
FusionCare Torrance
Spartan Clinic
Zion Clinic

7 locations selected

11_Reports Page

Overview: In addition to the reports that SPHER users are able create on the Events Page and Logs Page, SPHER users are able to create additional reports on the Reports Page.

The reports available on the Reports Page are as follows:

1. Audit Log Upload Report – This report displays information relating to the audit logs that have been uploaded and reviewed by SPHER.
   - The information contained within this report include:
     - Date which the file was reviewed
     - Date range of which the audit log file covers
     - Number of records (lines of captured user activity) within the audit log file
     - EHR/system of which the audit log file was generated from
   - Examples of use:
     - For medical groups uploading audit logs to SPHER manually, a user may want to check the date of when the last file was uploaded and the date range contained within that file before uploading a new file.
     - For medical groups whose EHR/system is capable of automatically uploading audit logs to SPHER, a user may want to troubleshoot whether this functionality within their EHR/system has failed to upload and when the failure first occurred.
2. Event Report – This report displays events captured in SPHER and their resolution.
   - The information contained within this report include:
     - Event Timestamp (date and time the event occurred)
     - Incident Code (unique code for the event)
     - Affected Location (location within the organization where the access too place)
     - Date Discovered (date the event was detected)
     - Detector (name of the Activity Detector that detected the event)
     - Individual/Entity (name of the individuals/entities who accessed the patient record)
     - Patients (name of the patients whose records were accessed)
     - Resolution Date (date the event was resolved in SPHER, date is blank if unresolved)
     - Status (current event status, e.g. “To Confirm,” “Pending,” etc.)
   - Examples of Use:
     - Within Excel, a user may want to generate a graph that captures the number of events detected by SPHER per day through the creation of a pivot table.
     - A user may want to search for a specific EHR user or patient and determine how many events detected by SPHER he or she was involved.
3. VIP Access Report– This report displays the activity (audit logs) of users that have accessed the medical record of a VIP patient.
   - The information contained within this report include:
     - Activity Timestamp (date and time the access to a VIP record occurred)
     - Location (location within the organization where the access took place)
     - User (name of the user who accessed the VIP record)
     - Role (user’s role within the organization, ex. Admin, Doctor, Nurse)
     - Action/Data (the specific action the user performed on the EHR while accessing the VIP’s medical record)

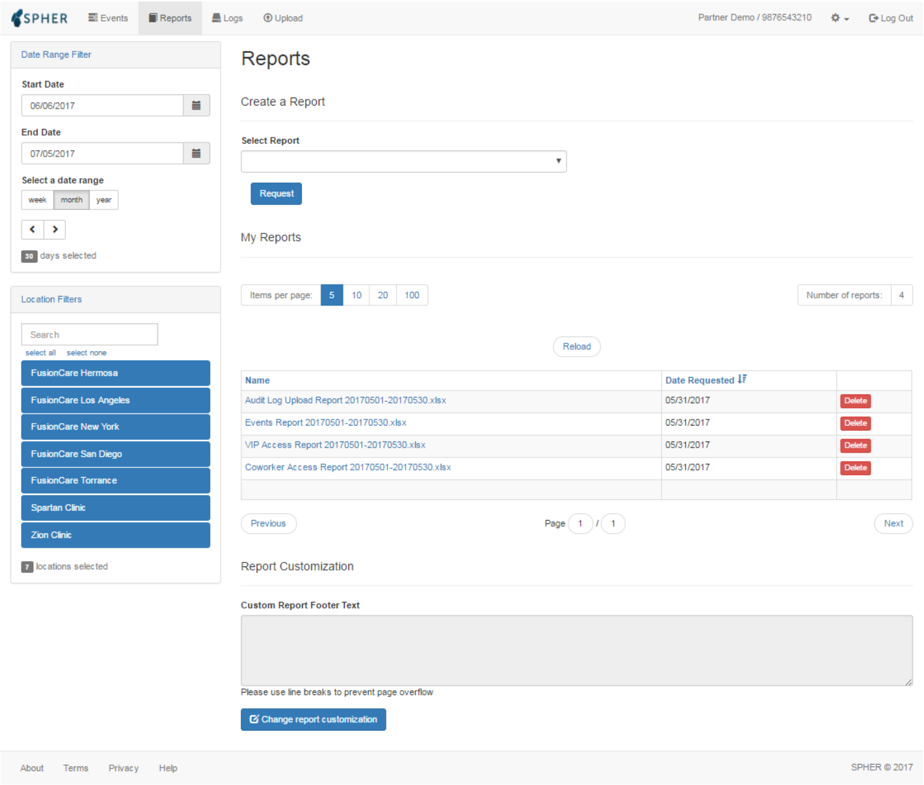
4. Coworker Access Report– This report displays the activity (audit logs) of users that have accessed the medical record of a coworker.
    - The information contained within this report include:
        - Activity Timestamp (date and time the access to a coworker record occurred)
        - Location (location within the organization where the access took place)
        - User (name of the user who accessed the coworker record)
        - Role (user's role within the organization, ex. Admin, Doctor, Nurse)
        - Action/Data (the specific action the user performed on the EHR while accessing a coworker's medical record)

To generate a report, follow the steps below:

Step 1: Go to **dashboard.amsspher.com** and log in to your SPHER account

Step 2: Go to **Reports page**

Step 3: Use the **Date Range Filter** on the left side bar to select the date range of the report you want to generate. You can also use the **Location Filters** on the left side bar to select the locations you want in the report.



Date Range Filter

Start Date: 06/06/2017

End Date: 07/05/2017

Select a date range: week [✓ month] year

30 days selected

Location Filters

- FusionCare Hermosa
- FusionCare Los Angeles
- FusionCare New York
- FusionCare San Diego
- FusionCare Torrance
- Spartan Clinic
- Zion Clinic

7 locations selected

Reports

Create a Report

Select Report

My Reports

Items per page: [✓ 5] 10 20 100

Number of reports: 4

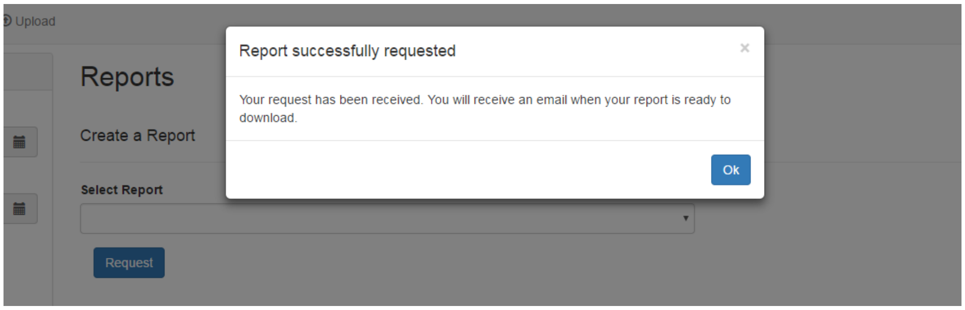
Name	Date Requested	
Audit Log Upload Report 20170501-20170530.xlsx	05/31/2017	Delete
Events Report 20170501-20170530.xlsx	05/31/2017	Delete
VIP Access Report 20170501-20170530.xlsx	05/31/2017	Delete
Coworker Access Report 20170501-20170530.xlsx	05/31/2017	Delete

Report Customization

Custom Report Footer Text

Please use line breaks to prevent page overflow

Step 4: Click the **Select Report** dropdown located at the top of the Reports Page and click on the **Report** that you wish to generate. Once the desired report is selected, click the **Request** button. A popup window will appear indicating that your request has been received. Once a report has been generated, it will be available in the **My Reports** table.

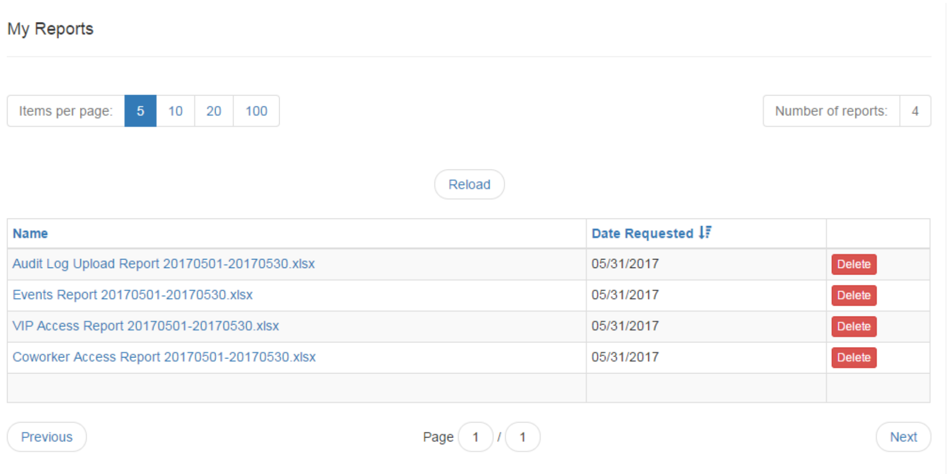


Report successfully requested

Your request has been received. You will receive an email when your report is ready to download.

Note: *The length of time a report takes to be generated will vary depending on the date range and the type of report selected. SPHER will send out an email for each requested report as soon as the report has been generated and made available in My Reports.*

Step 5: To open a report, click the name of the appropriated report in the **My Reports** table. By default, the My Reports table is sorted by the date the report was requested, with the most recently requested report appearing first.



Name	Date Requested ↓	
Audit Log Upload Report 20170501-20170530.xlsx	05/31/2017	Delete
Events Report 20170501-20170530.xlsx	05/31/2017	Delete
VIP Access Report 20170501-20170530.xlsx	05/31/2017	Delete
Coworker Access Report 20170501-20170530.xlsx	05/31/2017	Delete