HIPAA audit controls

You might need an overarching view of user activities when doing the following:

- Complying with the HIPAA Security Rule for ePHI

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
- Endpoint data
- Database data
- Medical device data

Example

In a healthcare organization, you must implement hardware, software, and procedural mechanisms to record and examine access and other activity in information systems that contain or use electronic protected health information (ePHI). These searches show who accessed patient health records, when they accessed them, and what activities they performed. In addition, they highlight unusual events such as failed password attempts and user accounts with excessive activity. This information can help your organization monitor suspicious users or activities before any data breach occurs.

To optimize the searches shown below, you should specify an index and a time range. These sample searches use Cerner audit logs. You can swap out this data source for ones in use at your organization, changing field names as necessary.

Timeline of access events

To see a timeline of which users accessed your system, organized by event type, run the following search.

```
sourcetype=Cerner_Audit_Log
PrsnlName=* | timechart count(UserName) BY EventType useother=false
```
Users patient record actions by event type

To see what actions your users have performed on patient records, run the following search.

```
sourcetype=Cerner_Audit_Log (EventType=Modify OR EventType=View* OR EventType=Security) 
ParticipantName=* PrsnlName=* 
| stats count BY EventName EventName PrsnlName 
| appendpipe [stats count BY PrsnlName EventType | rename EventName AS target, PrsnlName AS source] 
| appendpipe [stats count BY EventType EventName|rename EventType AS source, EventName AS target ] 
| search source=* 
| fields source target count
```

Number of failed logins by user ID

To count the number of failed logon attempts to a device, sorted by user ID, run the following search.

```
sourcetype=Cerner_Audit_Log AuditSource=* 
EventName="Logon Attempt" 
OutcomeInd="8" 
| stats count BY UserName 
| sort -count 
| rename UserName AS "User ID", count AS "Count"
```

Timeline of failed logins

To see a timeline of failed logins to your system, update the search to the following.

```
sourcetype=Cerner_Audit_Log AuditSource=* EventName="Logon Attempt" OutcomeInd="8" 
|fields _time,UserName 
| timechart count(UserName) BY UserName
```

System access information

To get a table of basic user activity information on your system, run the following search.

```
sourcetype=Cerner_Audit_Log 
PrsnlName=* 
| table _time, UserName, PrsnlName, Role, EventType, EventName, Application, NetworkAccID 
| convert ctime(_time) 
| rename _time AS "Time Accessed", UserName AS "User ID", PrsnlName AS "Name", EventType AS "Event Type", EventName AS "Event Name", NetworkAccID AS "Workstation"
```

Result

After running these access controls and taking appropriate action, you may want to look into other HIPAA controls:

---

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
- Access controls
- Integrity controls
- Person or entity authentication
- Transmission security