HIPAA access controls

In a healthcare organization, you must implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4)[Information Access Management]. These searches help you audit those policies and procedures.

Required data

- Endpoint data
- Medical device data

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

Unique user identification

To obtain a list of each user who logs into your system, run the following search.

```
sourcetype="cerner_audit_log"
  | stats dc(UserName)
```

Timeline of access activity by type

To see a timeline of user events, run the following search.

```
sourcetype=Cerner_Audit_Log
  PrsnlnName=* 
  | timechart count(UserName) BY EventType useother=f
```

Privileged user access activity

To see which of your privileged users have logged into a system, run the following search.

```
sourcetype="cerner_audit_log" NetworkAccID="*" ParticipantName="*" Role="*
  | lookup a Role AS Role
  | search priv=1
  | timechart count BY UserName useother=f
```
Privileged user access activity log

To obtain basic activity information on your privileged users, run the following search.

```
sourcetype=Cerner_Audit_Log PrsnlName=* NetworkAccID=*  
|lookup a Role AS Role  
|search priv=1  
|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"
```

Concurrent users at a single workstation

To see when more than two users are using a single workstation, run the following search.

```
sourcetype="cerner_audit_log"  
|streamstats dc(UserName) AS ConcurrentUsers BY NetworkAccID  
|where ConcurrentUsers>2  
|stats dc(UserName) AS "Unique Users" BY NetworkAccID  
|rename NetworkAccID AS "Workstation"
```

Next steps

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

- Audit controls
- Integrity controls
- Person or entity authentication
- Transmission security