HIPAA authentication controls

In a healthcare organization, you must implement procedures to verify the authenticity of a person or entity seeking access to electronic protected health information (e-PHI). These searches show whether credentials entered into an information system match those stored in that system and, if the user is authenticated, whether the person was granted the authorized access privileges to perform functions and access e-PHI.

Required data

- Medical device data

To optimize the searches shown below, you should specify an index and a time range. In addition, 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.

How to use Splunk software for this use case

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

```
sourcetype=Cerner_Audit_Log
AuditSource=*  
EventName="Logon Attempt"
OutcomeInd="8"
| stats count
```

To sort these results by user ID, update the search to the following.

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

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

```
sourcetype=Cerner_Audit_Log
AuditSource=*  
EventName="Logon Attempt"
OutcomeInd="8"
| bin _time span=5m
| fields _time,UserName
| timechart count(UserName) BY UserName
```
Next steps

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

- Access controls
- Audit controls
- Integrity controls
- Transmission security