HIPAA transmission security

In a healthcare organization, you must implement technical security measures that guard against unauthorized access to e-PHI being transmitted over an electronic network. You need to monitor server logs and email logs within your organization's environment to detect if protected health information is exposed to an unsecured environment. These searches alert relevant personnel if exposed PHI was detected so that the problem point can be identified and further data breach can be prevented.

Required data

- Endpoint data
- Medical device data

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

Transmission statistics

To run the following searches, you must have installed and configured the Splunk App for Stream.

Total number of transmission events

To count the number of e-PHI transmission events, run the following search.

```
sourcetype=stream:* | stats count AS Total
```

Number of events with exposed PHI

To count the number of e-PHI transmission events with exposed PHI, run the following search. You can remove any of the data points in the search below that aren't relevant to your system, or add others as needed.

```
sourcetype=stream:* (HL7_Tag=* OR (SSN=* OR card_details=*)) OR ((first_name1=* OR last_name=* OR names=*) AND (DOB=* OR ip_address=* OR phone_number=* OR street_address=*)) | stats count
```

Percentage of events with exposed PHI

To calculate the percentage of e-PHI transmission events that involved exposed PHI, run the following search. You can remove any of the data points in the search below that aren't relevant to your system, or add others as needed.

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.
Outbound PHI data by destination email

To see the destinations that each distinct source IP address is sending mail to, run the following search.

```
sourcetype=stream:* | stats dc(src_ip)
```

Emails with exposed PHI path

To see the receivers of emails that included exposed e-PHI transmission, run the following search. You can remove any of the data points in the search below that aren't relevant to your system, or add others as needed.

```
sourcetype=stream:smtp SSN=* OR HL7_tag=* OR street_address=* OR phone_number=* | stats count BY sender_email, receiver_email | rename receiver_email AS RECEIVER
```

Statistics from health information technology services, devices, and hardware

These sample searches use Cerner. You can swap out this data source for ones in use at your organization, changing field names as necessary.

Number of exported patient records

To see a count of the number of exported patient records, run the following search.

```
sourcetype=Cerner_Audit_Log EventType="Output" ParticipantName=* UserName=* | stats count
```

Modification events

To see the details of healthcare records that have been modified, run the following search.

```
sourcetype=cerner_audit_log EventType="Write/Update Results" OR EventType="Add" OR EventType="Sign" OR EventType="Modify" OR EventType="Modify Details" OR EventType="Add/Modify and Review"
```

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.
| convert ctime(_time) | table _time, EventType, UserName, PrsnlName, Role, EventName, NetworkAccID |
| rename _time AS "Date/Time", UserName AS "User ID", PrsnlName AS "Name", EventType AS "Event Type", EventName AS "Event Name", NetworkAccID AS "Workstation"

**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](#)
- [Person or entity authentication](#)