

## **Compliance Review Related to Loss of Portable Device**

**Reason for review:** Loss of laptop containing electronic protected health information (EPHI)

**Type of entity reviewed:** Covered Health Care Provider: Hospital

OESS received a complaint against a hospital related to a lost laptop that contained the electronic protected health information (EPHI) of several thousand patients. The hospital cooperated in investigating and resolving the complaint in an efficient manner. After closure of the case, OESS decided to conduct an onsite compliance review to assess the organization's overall compliance with the Security Rule. As part of this review, OESS placed particular emphasis on evaluating the policies and procedures related to offsite access and use of EPHI from remote locations or for the storing of EPHI on portable devices or media.

The Compliance Officer of the hospital verified that immediately after receiving notification of the complaint about the laptop loss, an inventory of all portable devices and media used by its workforce members was compiled and is routinely updated. In addition, the organization updated policies and procedures to verify that employees who used such devices with EPHI on them were knowledgeable about their responsibilities to keep it secure.

During the compliance review, pertinent IT and administrative staff were interviewed extensively. Documents, including the corrective action plan specific to the complaint, the risk assessment and risk management plan, as well as security policies and procedures were reviewed. The on-site compliance review identified other vulnerabilities and risks for the hospital, which included a lack of certain policies and procedures – for example, a policy and related procedures requiring a regular review to verify that workforce members have the appropriate level of systems access privileges necessary for their role within the organization. The review also revealed that the hospital had delays in the process for terminating access privileges for individuals no longer employed by the organization.

Following the review, the hospital developed a corrective action plan which included specific actions and a schedule for completion. Highlights from the initial corrective action plan, and the one following the compliance review are provided here:

- Implementation of additional physical security measures for the areas affected by the (lost laptop) incident to include 24 hour video surveillance and recording;
- Development and deployment of policies and procedures to ensure daily notification to the Information Technology department of any user that had been terminated;
- Implementation of a process to verify that access privileges are assigned in a manner that is consistent with the employee's role within the organization;

- Development and deployment of policies and procedures requiring laptops to be physically secured to the workstation where they are located and;
- Implementation of targeted information security training for all employees who use portable devices and media.

CMS determined that the corrective action plan, when fully implemented, would satisfactorily resolve the compliance issues underlying the complaint and those identified during the on-site review. CMS will monitor the plan for six months, at which time all actions are expected to be complete.

## **Compliance Review Related to Theft of Backup Tapes**

**Reason for Review:** Theft of backup tapes containing electronic protected health information (EPHI)

**Type of Entity Reviewed:** Covered Health Care Provider: Hospital

OESS received a complaint against a hospital related to a theft of backup tapes taken while en route to an offsite storage location. These tapes contained EPHI from thousands of patients. OESS decided to conduct an onsite review to assess the organization's overall compliance with the Security Rule. As part of this review, OESS placed particular emphasis on evaluating the policies and procedures related to storage of EPHI on backup devices and media and disposal of backup tapes containing EPHI.

The theft occurred when the contractor van, containing the backup tapes from the hospital, stopped to make a pickup. The contractor notified the hospital of the theft two days later. The hospital organized a crisis management team and identified what information was on the tapes and the level sophistication required for unauthorized parties to access the information. Additionally, the crisis management team terminated the relationship with the offsite storage contractor, temporarily created an offsite storage location for the backup tapes, and began encrypting backup tapes.

During the review, CMS interviewed pertinent IT and administrative staff. CMS reviewed documents, including the corrective action plan specific to the complaint, the risk analysis, business associate agreements, security training, and security policies and procedures. The on-site review identified gaps in their security awareness training program.

Following the review, the hospital developed a corrective action plan which included specific actions and a schedule for completion. The hospital also provided CMS with revised security procedures. Highlights from the initial corrective action plan, and the updated plan following the review are provided below:

- Implementation of encryption on all backup tapes which contain EPHI;

- Modification to the tape backup process to reduce the amount of EPHI transported on a daily basis;
- Termination of offsite storage contract and reevaluation of contactor requirements to transport and store backup tapes;
- Improvements to the new employee security awareness training program to require evidence of security awareness training prior to granting access to EPHI;
- Improvements to the refresher security awareness program to identify a specific frequency for refresher training and a process to verify that training had occurred;
- Creation of procedures to track disposed devices and degauss them prior to destruction; and
- Updates to the periodic policy and procedure review process to define a review timeframe for these documents.

CMS determined that the corrective action plan, when fully implemented, would satisfactorily resolve the compliance issues underlying the complaint and those identified during the on-site review. Post script: CMS monitored implementation of the plan, and confirmed that all steps had been completed.

## **Compliance Review Related to Theft of Workstation and Backup Hard Drive**

**Reason for Review:** Theft of workstation and backup hard drive containing electronic protected information (EPHI)

**Type of Entity Reviewed:** Covered Health Care Provider: Hospital

The HHS Office for Civil Rights (OCR) received a complaint against a hospital related to a theft of a workstation and backup hard drive from an office within the hospital. These devices contained personally identifiable information (PII) from thousands of patients. OCR referred the complaint to OESS based on the potential for violations of the HIPAA Security Rule. Based on this referral and subsequent evaluation of the facts surrounding the complaint, OESS decided to conduct an on-site review to assess the organization's overall compliance with the Security Rule. As part of this review, OESS placed particular emphasis on evaluating the policies and procedures related to storage of EPHI on workstations and portable devices, data encryption, and physical security. Additionally, CMS coordinated with OCR to assist OCR in conducting a review related to privacy concerns at the hospital. CMS worked closely with the hospital in detailing the event and their response, as there had been significant changes in the hospital's personnel since the incident occurred.

The theft occurred on a weekend within a leased office space, and therefore was not discovered until the following week. When discovered, the theft was immediately reported to the hospital's security office and to the police department. The incident response team at the time analyzed the situation and determined the type of information that was on the workstation and hard drive. Additionally, the organization updated policies and procedures, instructing employees that EPHI was not to be stored on

workstations or portable devices, and improved the physical security in the location of the theft.

During the review, CMS interviewed pertinent IT and administrative staff. CMS reviewed documents, including the corrective action plan specific to the complaint, the risk analysis, and security training as well as security policies and procedures. The on-site review identified other vulnerabilities and risks for the hospital, which included a lack of certain policies and procedures - for example, a policy and related procedures on performing periodic risk assessments.

Following the review, the hospital developed a corrective action plan which included specific actions and a schedule for completion. Highlights from the initial corrective action plan, and the updated plan following the review are provided below:

- Implementation of enhanced physical security measures for the area affected by installing and monitoring electronic card key access;
- Development and deployment of policies and procedures requiring EPHI to be stored on network servers and not stored on individual workstations or portable devices;
- Implementation of a formalized, documented risk assessment process aligned with the [HHS “Basis of Risk Analysis and Risk Management”](#) and the [National Institute of Standards and Technology Special Publication 800-30, “Risk Management Guide for Information Technology Systems”](#);
- Development and deployment of policies and procedures on whole disk encryption, with a roll-out schedule based on identified risk;
- Improvements to the policy and procedure review process; and,
- Development and deployment of policies and procedures for the security training process.

CMS determined that the corrective action plan, when fully implemented, would satisfactorily resolve the compliance issues underlying the complaint and those identified during the on-site review. CMS will monitor the plan for two years, at which time all actions are expected to be complete.

## **Compliance Review Related to Theft of Laptop**

**Reason for Review:** Theft of a laptop containing electronic protected health information (EPHI)

**Type of Entity Reviewed:** Covered Health Care Provider: Hospital

OESS became aware of an incident at a hospital related to the theft of a laptop containing EPHI from the residence of the hospital’s contractor. The laptop reportedly contained information from a large number of the hospital's former patients, employees, and physicians. OESS decided to conduct an on-site review to assess the organization's overall compliance with the Security Rule. As part of this review, OESS placed particular

emphasis on the implementation of policies and procedures that address EPHI storage on portable devices and media, off-site access, and use of EPHI from remote locations.

The theft occurred when a hospital-supplied laptop computer was stolen from the residence of a hospital contractor. The contractor notified the hospital's security officer, who assembled the hospital's incident response team. The security officer compiled the information that may have been stored on the stolen laptop. Unknown to the hospital, the contractor had been copying EPHI data to the laptop, which was in violation of the hospital's policy on the storage of EPHI. As a result of this incident, the business associate agreement with the contractor was terminated by the hospital. In addition, the hospital implemented whole disk hard drive encryption software on all laptops. The security officer reviewed all security policies and procedures and provided re-education to hospital leadership on EPHI safeguards and policies. The hospital also put in place a mandatory annual security awareness training program. Additionally, the hospital configured laptops used off-site to receive only the minimum information required for each day's work and wipe the data each night after the user remotely accessed the hospital's network.

During the review, CMS interviewed pertinent IT and administrative staff. CMS reviewed documents, including the corrective action plan specific to the complaint, the risk analysis, business associate agreements, security training, and security policies and procedures. The on-site review identified compliance gaps with the hospital's risk assessment, sanctions policy, , security awareness training program, , and physical security mechanisms to protect workstations. Additionally, CMS noted that while policies existed, in some cases the procedures were not documented, so the policies were not implemented consistently.

Following the review, the hospital developed a corrective action plan, which included specific actions and a schedule for completion. Highlights from the initial corrective action plan, and the updated plan following the review are provided below:

- Termination of the business associate agreement with the contractor;
- Implementation of whole disk hard drive encryption software on all laptops;
- Review of security policies and procedures and re-education for hospital leadership on EPHI safeguards and policies;
- Implementation of a mandatory annual security awareness training program;
- Reconfiguration of the daily work process to reduce the amount of EPHI stored on off-site laptops;
- Implementation of a formalized, documented risk assessment process aligned with the [HHS "Basis of Risk Analysis and Risk Management"](#) and the [National Institute of Standards and Technology Special Publication 800-30, "Risk Management Guide for Information Technology Systems"](#) and covering all applications that store, process, or transmit EPHI;
- Development of an updated process for account provisioning that more tightly integrates employees' completion of initial training with account provisioning;
- Periodic self-audits of employee compliance with training requirements;

- Implementation of sanctions for employees who are non-compliant with security awareness training requirements;
- Implementation of procedures and tools to support physical safeguard policies; and
- Implementation of a system configuration management process.

CMS determined that the corrective action plan, when fully implemented, would satisfactorily resolve the compliance issues underlying the complaint and those identified during the on-site review. Post Script: the entity completed the Corrective Action Plan and all items have been verified in follow up discussions and document reviews.

## **Compliance Review Related to Theft of Laptop**

**Reason for Review:** Loss of laptop containing electronic protected health information (EPHI)

**Type of Entity Reviewed:** Covered Health Care Provider: Emergency Medical Service (EMS)

OESS became aware of an incident at an emergency medical service (EMS) department related to the loss of a laptop. The laptop contained EPHI from several hundred patients and personally identifiable information (PII) from several thousand EMS personnel. OESS decided to conduct an onsite review to assess the organization's overall compliance with the Security Rule. As part of this review, OESS placed particular emphasis on evaluating the policies and procedures related to storage of EPHI on portable devices and media, off-site access, and use of EPHI from remote locations.

EMS personnel left the laptop in the emergency room docking station after transferring a patient to hospital care. When the EMS personnel returned a few hours later, the laptop was not in the docking station and could not be located. EMS, with the assistance of their information systems department, identified the information that was on the missing laptop. After the incident, EMS removed all outdated patient data from their laptops. Additionally, EMS installed whole disk encryption software on all of their laptops.

During the review, CMS interviewed pertinent IT and administrative staff. CMS reviewed documents, including the corrective action plan specific to the complaint, physical security controls and security training as well as security policies and procedures. The on-site review identified compliance gaps which included a lack of certain security related policies and procedures, outdated policies and procedures, and the lack of a risk assessment. CMS provided guidance to EMS on establishing a baseline of compliance to the HIPAA Security Rule, recognizing EMS's limited resources. As part of this baseline compliance plan, CMS recommended that the organization engage a third party to conduct a gap analysis and assist the organization in developing policies and procedures to aid them in meeting Security requirements.

Following the review, the EMS department developed a corrective action plan which included specific actions and a schedule for completion. Highlights from the initial corrective action plan, and the updated plan following the review are provided below:

- Formally requested that an application vendor make improvements to the password controls on software;
- Implement an automated process to remove outdated EPHI from laptops on a daily basis;
- Implementation of whole disk encryption software on all the EMS laptops;
- Development and deployment of policies and procedures on granting access to the network and applications;
- Development and deployment of policies and procedures on password controls;
- Development and deployment of policies and procedures on encryption and decryption of EPHI;
- Development and deployment of policies and procedures on the initial and refresher security training program;
- Implementation of a formalized, documented risk assessment process aligned with the [HHS “Basis of Risk Analysis and Risk Management”](#) and the [National Institute of Standards and Technology Special Publication 800-30, “Risk Management Guide for Information Technology Systems”](#) and covering all applications that store, process, or transmit EPHI;
- Improvements to the policy and procedure review and approval process; and,
- Improvements to the initial security awareness training program.

CMS determined that the corrective action plan, when fully implemented, would satisfactorily resolve the compliance issues underlying the complaint and those identified during the on-site review. Post script: CMS monitored implementation of the plan, and confirmed that all steps had been completed.

## **Compliance Review Related to a Computer Virus Infection**

**Reason for Review:** Organization’s Computer System Infected by a computer virus – risk of exposure of personally identifiable information (PII)

**Type of Entity Reviewed:** Covered Health Care Provider: Healthcare Organization

OESS became aware of an incident at a healthcare organization related to a computer virus infection from an unknown source that infected the organization's computer systems. The virus exposed personal health information (PHI) on individuals who made financial contributions to the organization, as well as employee usernames and passwords. OESS decided to conduct an on-site review to assess the organization's overall compliance with the Security Rule. As part of this review, OESS placed particular emphasis on the implementation of technical safeguards, as well as policies and procedures that address virus identification and protection of data. .

The infection occurred when the virus entered the network via an unknown origin, potentially through a workstation connected to the organization's internal network. The virus exploited a vulnerability in the organization's anti-virus software which allowed it to terminate the software and execute malicious code on the organization's workstations and servers. Because of the exploited anti-virus software, a second virus was able to infect another server that stored donor credit card information. The organization's information technology command center, noticing a decline in the network's performance, proceeded to investigate and block network traffic for services exploited by the virus. Additionally, the organization employed a forensic software analyst to determine the scope of the damage, vulnerabilities exploited, and the nature of the viruses responsible for the breach. The analysis determined that the virus exposed employee usernames and passwords. However, the analysis concluded that the virus did not expose protected health information.

During the review, CMS interviewed pertinent IT and administrative staff. CMS reviewed documents, including the corrective action plan specific, the risk analysis, security training, virus protection and updating mechanisms, and security policies and procedures. The on-site review identified compliance gaps with the organization's risk assessment, security awareness training, incident detection, reporting, and response, and anti-virus protection. CMS also noted that firewalls were not installed or enabled on laptops used to remotely access the organization's network. Finally, CMS identified a number of required policies and procedures that had not been created or deployed. . CMS recommended that the organization conduct a gap analysis to assist the organization in developing additional policies and procedures to aid them in meeting compliance requirements.

During the course of the review, the organization identified areas in which they struggled with compliance which were outside of the scope of the review. CMS provided additional guidance in these other areas to help the organization drive continued compliance.

Following the review, the organization developed a corrective action plan, which included specific actions and a schedule for completion. Highlights from the initial corrective action plan, and the updated plan following the review are provided below:

- Reset of all passwords exposed by the virus;
- Improvement over the management and implementation of anti-virus software;
- Establishment of a working group to aid in identifying assets that store, process, or transmit EPHI;
- Identification of ownership for assets that store, process, or transmit EPHI;
- Development of policies and procedures to document existing processes and support identified gaps in documentation required for HIPAA compliance;
- Improvement in the process for conducting new employee security awareness training including requiring evidence of security awareness training prior to granting access to EPHI;
- Implementation of temporary audits of new training procedures to verify compliance;

- Consolidation of incident tracking mechanisms and development of procedures to support centralized tracking;
- Implementation of personal firewall software and increased use of centralized management tools for malicious software protection; and,
- Implementation of stronger wireless network encryption.

CMS determined that the corrective action plan, when fully implemented, would satisfactorily resolve the compliance issues underlying the complaint and those identified during the on-site review. CMS monitored implementation of the plan, and confirmed that all steps had been completed.

## **Compliance Review Related to Theft of Workstation and Backup Hard Drive**

**Reason for Review:** Unauthorized disclosure of protected health information (EPHI)

**Type of Entity Reviewed:** Covered Health Care Provider: Pharmacy

The HHS Office for Civil Rights (OCR) received a complaint against a pharmacy related to unauthorized disclosure of prescription information. OCR referred the complaint to OESS based on the potential for violations of the HIPAA Security Rule. Based on this referral and subsequent evaluation of the facts surrounding the complaint, OESS initiated contact with the pharmacy to resolve the complaint. Based on information provided by the pharmacy, OESS determined that monitoring controls in place at the organization may not have reasonably protected against potential further breaches of EPHI. Based on this evaluation, OESS decided to conduct an on-site complaint investigation to assess the organization's overall compliance with the HIPAA Security Rule. As part of this review, OESS placed particular emphasis on policies and procedures that addressed monitoring of access to EPHI as well as access and use of EPHI from remote locations.

Representatives from the pharmacy verified that after receiving information regarding the potential unauthorized disclosure, they investigated the issue and discussed it with relevant parties. Their evaluation determined that no further action was necessary and that existing monitoring controls were reasonable and appropriate for their environment.

During the complaint investigation, CMS interviewed pertinent IT and administrative staff. CMS reviewed documents, including the pharmacy's risk analysis, access control policies, training policies, and employee screening policies. The on-site complaint investigation identified other vulnerabilities and risks to the pharmacy, which included, but were not limited to, a lack of timely training for new employees stemming from a large influx of new employees, gaps in the screening process for new employees stemming from a the same influx, and failure to review users' assigned access levels on a periodic basis.

At the conclusion of the review, CMS worked with representatives from the pharmacy to revise the reporting process to allow the pharmacy to provide their detailed responses alongside the identified gaps. This change in report structure provided a more effective format to integrate the pharmacy's responses into the reporting process.

Following the review, the pharmacy developed a corrective action plan which included specific actions and a schedule for completion. Highlights from the corrective action plan developed following the complaint investigation are provided below:

- Evaluation of the existing training program to identify and implement necessary modifications;
- Revisions of the hiring process to improve compliance with screening requirements;
- Updates to access procedures to improve the effectiveness of modifications to user access; and,
- Development of formalized device disposal policies and procedures.

CMS determined that the corrective action plan, when fully implemented, would satisfactorily resolve some of the compliance issues identified during the on-site review. Post script: CMS monitored implementation of the plan, and confirmed that all steps had been completed.