CANCER CENTER PORTABLE DEVICES:
INVESTIGATION OF ALLEGATIONS

THE UNIVERSITY OF NEW MEXICO

Report 2015-14
October 9, 2014

Audit Committee Members
J.E. "Gene" Gallegos, Chair
Lt. General Bradley Hosmer, Vice Chair
James Koch

Audit Staff
Manu Patel, Internal Audit Director
Chien-Chih Yeh, Internal Audit Manager
Lisa Wauneka, IT Auditor
Avedona Lucero, Senior Auditor
CONTENTS

EXECUTIVE SUMMARY .................................................................................................................. 1
  BACKGROUND .......................................................................................................................... 1
  COMPLAINT SPECIFIC CONCLUSION ..................................................................................... 1
  CONCLUSION .......................................................................................................................... 2

INTRODUCTION .......................................................................................................................... 3
  BACKGROUND .......................................................................................................................... 3
  PURPOSE ................................................................................................................................... 3
  PROCEDURES ........................................................................................................................... 3

OBSERVATIONS, RECOMMENDATIONS AND RESPONSES ......................................................... 4
  INCIDENT LOG .......................................................................................................................... 4
  TIMELY REMOVAL OF PHI FROM USB .................................................................................. 4
  ADEQUATE PROTECTION OF INFORMATION ON USB’S – ENCRYPTION ............................ 5
  USB INVENTORY ...................................................................................................................... 6
  ARCHIVED PHI ......................................................................................................................... 7
  COMPLAINT SPECIFIC CONCLUSION ..................................................................................... 8

APPROVALS .................................................................................................................................... 10

ABBREVIATIONS

CC ......................................................................................................................... University of New Mexico Cancer Center
CD ......................................................................................................................... Compact Disc
HSC ......................................................................................................................... Health Sciences Center
IT ............................................................................................................................. Information Technology
PACS ......................................................................................................................... Picture Archiving and Communicating System
PHI ......................................................................................................................... Protected Health Information
RO ............................................................................................................................. Radiation Oncology
UNM ......................................................................................................................... University of New Mexico
UNMH ......................................................................................................................... University of New Mexico Hospital
USB ............................................................................................................................. Universal Serial Bus
EXECUTIVE SUMMARY

BACKGROUND

This investigation originated from a report to the UNM Hotline. The report referenced two incidents in which portable devices were lost or misplaced. In one instance, the person reporting stated that it involved a Universal Serial Bus (USB) Flash Drive. In another, the device was one or more compact discs (CDs).

TIMELY REMOVAL OF PHI FROM USB

The CC does not always clear Protected Health Information (PHI) from USB Flash Drives. They do not delete all information from them immediately after transferring PHI from one computer to the next, as they should do per oral instruction of the Radiation Oncology department (RO).

The Chief Financial Officer of the CC should work with the HSC Information Technology (IT) Security Office to ensure that they develop procedures relating to proper use of portable devices. Procedures should require, but not be limited to, erasure of data immediately following transference of information from one area to another. The Chief Financial Officer of the CC should communicate these procedures to all portable device users. In addition, the CC should monitor the process to ensure staff follow the correct procedures.

ADEQUATE PROTECTION OF INFORMATION ON USB’S – ENCRYPTION

The CC does not adequately protect information on USB flash drives via encryption, password protection or keypad entry protection. Outside entities could easily access the PHI on the unprotected USB flash drive should the USB flash drive be lost.

The Chief Financial Officer of the CC should work with HSC IT Security Office to ensure that they encrypt and password protect all portable devices.

COMPLAINT SPECIFIC CONCLUSION

It is difficult to determine the validity of the allegation that two CDs were missing in August 2013 (per the original complaint). This is due to the lack of a documented process for reporting, investigating, and forwarding of incidents to the HSC Privacy Officer.

A summary of CC investigative reports conducted by the HSC Privacy Officer from January 2010 through July 2014 noted thirty-five investigated instances; two of those instances related to missing portable devices.
EXECUTIVE SUMMARY

The Chief Financial Officer of the CC should formally assign the responsibility of managing portable devices, determining potential loss, managing the investigative process, reporting to the HSC Privacy Officer, and communicating the outcome to designated individuals at the CC as appropriate. The person responsible for overall oversight should develop written standard operating procedures for the process, communicate the standard operating procedures to all staff, and require annual training in compliance with HSC Policy 300.

CONCLUSION

The CC utilizes portable devices to transfer and archive PHI. Therefore, it is important that they implement procedures to ensure that all PHI is properly protected and that they follow standardized procedures for reporting, documenting, and communicating any/all incidents of missing portable devices.
INTRODUCTION

BACKGROUND

The Cancer Center (CC) utilizes portable Information Technology (IT) storage devices, Compact Discs (CDs) or Universal Serial Buses (USBs) flash drives, in various areas of operation. Protected Health Information (PHI) is stored on the portable devices on a permanent and temporary basis. The CC employs various methods for reporting missing portable devices from original discovery, to internal CC reporting, through to reporting to the HSC Privacy Officer.

This investigation originated from a report to the UNM Hotline. The report referenced two incidents in which portable devices were lost or misplaced. In one instance, the person reporting stated that it involved a Universal Serial Bus (USB) Flash Drive. In another, the device was one or more compact discs (CD’s).

PURPOSE

The purpose of this confidential report is to provide a summary of findings and recommendations made as a result of our investigation into the following allegations:

- Two instances of portable devices with Patient Health Information (PHI) on them reported missing;
- The unusually long period of time to investigate and report the missing devices to the appropriate HSC Privacy Officer; and
- A misreported discovery date - the actual discovery date was several months prior to the date the CC management reported to the HSC Privacy Officer.

PROCEDURES

Internal Audit interviewed key personnel at the CC and at the HSC Privacy Officer to obtain an understanding of their general use of USB flash drives and CDs, as well as procedures in place to report incidents of missing USBs or CD’s.
OBSERVATIONS, RECOMMENDATIONS AND RESPONSES

INCIDENT LOG

The CC does not keep an incident log to track any reported missing portable devices, thus creating difficulty with regard to tracking the incidents and outcomes. It is difficult to determine: if the CC reports all incidents to the HSC Privacy Officer; the timeline from time of report to investigation; and, the ultimate resolution of incidents. As a result, incidents may go unreported or may not be investigated thoroughly and in a timely manner.

In the case of a breach, HIPAA requirements include timely notice of a potential breach to any and all parties potentially affected.

Recommendation 1

The Chief Financial Officer of the CC should ensure that they develop a comprehensive log for reporting any missing portable devices. The log should include, at minimum, the date of discovery, the description of the item, the reporting party, and a running description of action taken through to the disposition. The Chief Financial Officer of the CC should assign responsibility to the appropriate level of management for use, follow-up and management of the log.

Response from the Chief Financial Officer of the CC:

<table>
<thead>
<tr>
<th>Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Targeted Completion Date:</strong> Effective date: April 1, 2015</td>
</tr>
<tr>
<td><strong>Assigned to:</strong> Chief Financial Officer</td>
</tr>
<tr>
<td><strong>Corrective Action Planned:</strong> UNM Cancer Center agrees with the recommendation. UNMCC will create a process and log to record incidents of missing portable devices. Key elements will include: date of discovery, relator, description of incident, description or unique identifier of unit lost, chain of communication (i.e. who incident was reported to), resolution of incident (i.e. re-inventory taken and media found, media not found; HIPPA Breach Notification Form completed and submitted appropriately).</td>
</tr>
</tbody>
</table>

TIMELY REMOVAL OF PHI FROM USB

The CC does not always clear Protected Health Information (PHI) from USB Flash Drives. They do not delete all information from them immediately after transferring PHI from one computer to the next, as they should do per oral instruction of the Radiation Oncology department (RO).
The practice, if consistently adhered to, will reduce the risk of losing PHI and minimize instances of reportable breach of information.

HSC policy HSC-266 “Device and Media Control applies to electronic media in any format that contains Confidential or Restricted information. Section HSC-260.2 Disposition and/or Disposal of Media containing Confidential or Restricted Information states the following:

Complete removal of Confidential or Restricted information from electronic media is required before the media is made available for re-use (Reference: Procedure HSC-260 PR.1).

Recommendation 2

The Chief Financial Officer of the CC should work with the HSC IT Security Office to ensure that the CC develops procedures relating to proper use of portable devices. They should require, but not be limited to, erasure of data immediately following transference of information from one area to another. The Chief Financial Officer of the CC should communicate these procedures to all portable device users. In addition, the CC should monitor the process to ensure staff follow the correct procedures.

Response from the Chief Financial Officer of the CC:

<table>
<thead>
<tr>
<th>Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Targeted Completion Date:</strong> Effective date: April 1, 2015</td>
</tr>
<tr>
<td><strong>Assigned to:</strong> Chief Financial Officer</td>
</tr>
<tr>
<td><strong>Corrective Action Planned:</strong> UNM Cancer Center agrees with the recommendation. UNMCC will work with HSC IT Security to develop procedure for the management and security of portable media used in UNM Cancer Center Radiation Oncology department. The procedure will include periodic review of processes to ensure compliance.</td>
</tr>
</tbody>
</table>

**Adequate Protection of Information on USB’s – Encryption**

The CC does not adequately protect information on USB flash drives via encryption, password protection or keypad entry protection. Outside entities could easily access the PHI on the unprotected USB flash drive should the USB flash drive be lost. Adding this precaution would reduce the risk of a breach of PHI should a portable device be lost and unrecovered.
HSC policy HSC-23C “Electronic Data Storage” establishes standards for the electronic transmission and storage of Confidential or Restricted information. Section HSC-230.2 Data in Storage and Data in Transit states the following:

Encryption of files, documents, and messages for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks, is encouraged at all times and may be required.

Recommendation 3

The Chief Financial Officer of the CC should work with the HSC IT Security Office to ensure that they encrypt all portable devices.

Response from the Chief Financial Officer of the CC:

<table>
<thead>
<tr>
<th>Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Targeted Completion Date:</strong> Effective date: April 1, 2015</td>
</tr>
<tr>
<td><strong>Assigned to:</strong> Chief Financial Officer</td>
</tr>
<tr>
<td><strong>Corrective Action Planned:</strong> UNM Cancer Center agrees with the recommendation. UNM Cancer Center will work with HSC IT Security to investigate solutions that will allow us to encrypt the USB drives used for transferring data between radiation oncology treatment systems. Key considerations with this solution will involve securing encryption capabilities that will be compatible with the proprietary software of the treatment planning systems.</td>
</tr>
</tbody>
</table>

**USB INVENTORY**

Per the USB flash drive assignment sheet, the number of USB flash drives in RO does not reconcile to the physical number of drives on hand. There was one more on hand than accounted for on the sign out sheet. The CC does not log or document PHI transferred via a portable device. Should a portable device be lost, it is left to personal memory to determine what information may have been on the device. The CC needs to inventory the USB flash drives and document the inventory process.

Absent a solid inventory process, it is impossible to be certain that all portable devices are accounted for or to monitor the transfer of PHI. Should a portable device with PHI on it go missing, it would go undetected. This results in a potential breach. In addition, it may not be possible to determine what exact PHI was on the portable device.
Observations, Recommendations and Responses

Recommendation 4:

The Chief Financial Officer of the CC should ensure that the CC develops an inventory process for portable devices and that they perform and document reconciliations at minimum on a monthly basis. The process should include a specific device assignment and/or check out system and ongoing documentation of information loaded onto and removed from each device by date.

Response from the Chief Financial Officer of the CC:

<table>
<thead>
<tr>
<th>Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Targeted Completion Date:</strong> Effective Date: April 1, 2015</td>
</tr>
<tr>
<td><strong>Assigned to:</strong> Chief Financial Officer</td>
</tr>
<tr>
<td><strong>Corrective Action Planned:</strong> UNM Cancer Center agrees with recommendation and will develop and document an inventory process to ensure management and security of portable devices including a timely inventory (at a minimum monthly) of devices.</td>
</tr>
</tbody>
</table>

ARCHIVED PHI

The need to store archived PHI on CD can potentially be eliminated by storing the information in the Picture Archiving and Communicating System (PACS) at UNMH. The current process includes storing PHI on a CD for the inactive patient. The PHI is archived on a CD in case the patient returns for future treatment. The CDs are occasionally retrieved for use if the patient returns for treatment or if archived information is requested by the patient or another physician.

The CDs are stored in a locked room in a safe and there is a sign out process. However, the process is not monitored and the CDs can be checked out for an indefinite period of time. This may result in the potential loss or misplacement of the CDs. Any loss of a CD may not be discovered for a long period of time.

Recommendation 5:

The Chief Financial Officer of the CC should explore the feasibility of using the PACS system for archiving information.
OBSERVATIONS, RECOMMENDATIONS AND RESPONSES

Response from the Chief Financial Officer of the CC:

<table>
<thead>
<tr>
<th>Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Targeted Completion Date:</strong> Effective Date: May 1, 2015</td>
</tr>
<tr>
<td><strong>Assigned to:</strong> Chief Financial Officer</td>
</tr>
<tr>
<td><strong>Corrective Action Planned:</strong> UNM Cancer Center will investigate the possibility of utilizing a PACS system for archiving ongoing treatment and planning data. In regards to existing archived storage on portable CDs, UNM Cancer Center is currently in the process of moving this data from the CD archives to a shared network folder. The transition of this data to the network folder to be completed by April 30, 2015. In regards to archived storage on tape media, an RFP to be issued for the permanent archive of this media from tape to a networked server/folder. To be completed by June 30, 2015.</td>
</tr>
</tbody>
</table>

Recommendation 6:

The Chief Financial Officer of the CC should ensure that the CD inventory documentation process includes a mandated maximum check out time and regular monitoring and reconciliation of CDs in the vault.

Response from the Chief Financial Officer of the CC:

<table>
<thead>
<tr>
<th>Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Targeted Completion Date:</strong> Effective Date: April 1, 2015</td>
</tr>
<tr>
<td><strong>Assigned to:</strong> Chief Financial Officer</td>
</tr>
<tr>
<td><strong>Corrective Action Planned:</strong> UNM Cancer Center agrees with recommendation and will develop and document an inventory process to ensure management and security of CDs, which would include a check out and inventory procedure.</td>
</tr>
</tbody>
</table>

COMPLAINT SPECIFIC CONCLUSION

A summary of CC investigative reports conducted by the HSC Privacy Officer from January 2010 through July 2014 noted thirty-five investigated instances; two of those instances related to missing portable devices. During the course of conducting the investigation, the HSC Privacy Officer informed Internal Audit there is a recent reported incident involving the loss of a CD from the Medical Records Department. That investigation is ongoing by the HSC Privacy Officer and it is anticipated that a notification letter(s) will be sent to the affected persons shortly.
The following is a summary of the details obtained from interviews and sporadic documentation, including informal email:

It is difficult to determine the validity of the allegation that two CDs were missing in August 2013 (per the original complaint) as opposed to the reported date of January 2014. This is due to the lack of a documented process for reporting, investigating, and forwarding of incidents to the HSC Privacy Officer.

Per the official report by the HSC Privacy Officer, the CD’s were originally reported as missing to a CC RO supervisor in fall 2013. At that time, CC staff conducted an informal search. The CC RO supervisor indicated that there was miscommunication, and the supervisor was under the impression that the CDs had been found. The official report lists January 2014 as the discovery date, not a date in the fall of 2013. Following through the documentation from the time that the HSC Privacy Officer was notified, and going with the January 2014 discovery date does not violate any HIPAA rules to timely reporting. The potentially affected parties were notified in accordance with HIPAA within the required time limits. However, the entire scenario does give ample support for the need for a documented standard operating Procedure and position specific chain of command with regard to missing portable device discovery and reporting.

Recommendation 7:

The Chief Financial Officer of the CC should formally assign the responsibility of managing portable devices, determining potential loss, managing the investigative process, reporting to the HSC Privacy Officer, and communicating the outcome to designated individuals at the CC as appropriate. The person responsible for overall oversight should develop standard operating procedures for the process, communicate the standard operating procedures to all staff, and require annual training in compliance with HSC Policy 300.

Response from the Chief Financial Officer of the CC:

<table>
<thead>
<tr>
<th>Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Targeted Completion Date:</strong> Effective Date: April 1, 2015</td>
</tr>
<tr>
<td><strong>Assigned to:</strong> Chief Financial Officer</td>
</tr>
<tr>
<td><strong>Corrective Action Planned:</strong> UNM Cancer Center will initiate a process ensure that staff are current on their required annual training supporting the handling of protected information such as HIPAA information. UNMCC will initiate a process to develop and train our staff on standard operating procedures for communicating and reporting incidents to the appropriate levels of authority in the institution. UNMCC has a dedicated Compliance Officer who maintains the responsibility for managing the investigative process, coordinating communication within UNMCC, and reporting to the HSC Privacy Officer.</td>
</tr>
</tbody>
</table>
APPROVALS

Manu Patel, CPA
Director, Internal Audit Department

Approved for Publication

Chair, Audit Committee