DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Risk Management and Incident Response
Incident Resolution Team

Monthly Report to Congress of Data Incidents

January 2 - February 5, 2012

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000070282	Mishandled/ Misused Physical or Verbal Information	VISN 04 Altoona, PA	1/3/2012	1/17/2012	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0539603	1/3/2012	INC000000190362	N/A	N/A	N/A	1	

Incident Summary

Veteran A was given the surgical discharge instructions that were intended for Veteran B. The discharge instructions contained Veteran B's name, full SSN, date of birth, and protected health information (PHI).

Incident Update

01/04/12:
Veteran B will be sent a letter offering credit protection services.

01/09/12:
The credit protection letter was prepared. The Privacy Officer (PO) will meet with Veteran B in person to deliver the letter and explain the incident and the purpose for the credit protection services.

NOTE: There were a total of 113 Mis-Handling incidents this reporting period. Because of repetition, the other 112 are not included in this report, but are included in the "Mis-Handling Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

The document was retrieved by the Privacy Officer. The credit protection letter was given to Veteran B. Education was provided to the OR staff by the Privacy Officer.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000070352	Missing/Stolen Equipment	VISN 01 Bedford, MA	1/5/2012	1/6/2012	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0540098	1/5/2012	INC000000190755	N/A	N/A	N/A		

Incident Summary

The Dietetic Service Chief reported that an unencrypted laptop was missing from her locked office. The laptop had the standard Bar Code Medication Administration (BCMA) image and some PowerPoint slides on diabetes control on it. She last used the device on 12/01/11 to provide staff education. After the class, she placed the laptop into the storage case which she kept in her locked office. She was on leave 12/14/11 - 01/02/12. The laptop case was in its place in her office when she returned to work. When she went to take the laptop out today for a class, she discovered that the laptop was not in the case. A VA Police report was filed.

Incident Update

01/06/12:
The laptop had the standard BCMA image installed on it. The Service Chief confirmed there was no personally identifiable information (PII) or protected health information (PHI) stored on it.

01/09/12:
The preliminary VA Police Service investigation indicates that there was no evidence of forced entry into the Service Chief's office and nothing else was taken or disturbed. The Service Chief and the Housekeeping staff have the only keys to the office. The VA Police have not had the opportunity to interview the Housekeeping staff yet. There are no cameras in the area. There is a VA Police Officer seated in the lobby about 50 feet from the Service Chief's office however there is another exit around the opposite corner from the office. The case has been forwarded to a VA Detective for further investigation.

01/26/12:
The interviews with the Housekeeping staff have been completed. The VA Police have no other leads at this time.

01/27/12:
This was a BCMA laptop. It was temporarily loaned to the employee because the regular system in the conference room was not available for use. The presentation given was for staff training and not for patients. The laptop did not contain any sensitive information.

Resolution

The Service Chief confirmed there was no PII or PHI stored on it.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000070437	Mishandled/ Misused Physical or Verbal Information	VISN 19 Denver, CO	1/5/2012		Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0540321	1/5/2012	INC000000190893	N/A	N/A	N/A	186	

Incident Summary

A VA employee from Home Based Primary Care left a box of information outside of Building 4 which contained documents including patients' names, full SSN, visit dates, diagnosis, addresses, phone numbers and patient inquiry information. The estimated number of Veterans affected by this incident is unknown. An exact count will be provided after assessing the entire box of documents and developing a list of patients affected. A VA Police Officer first noticed the box and took possession of it at 3:30 PM on 01/05/12. The Police Officer determined that the box belonged to Home Based Primary Care by looking at the content of the documents. The Police Officer contacted the Home Based Primary Care coordinator to ask if the box belonged to her and she acknowledged that it was hers. She informed the Police Officer that the box had been left unattended from about 8:00 AM to 3:30 PM.

Incident Update

01/06/12:
The employee used the box to transfer information from work to home. When bringing the box back into work one morning she set it down by the door outside the building then forgot it. The box contained records of 168 patients. Letters of credit protection services will be sent to 168 patients.

01/09/12:
After further review of the documents, the number of patients affected has been confirmed to be 186. The 186 patients will receive a letter offering credit protection services.

01/18/12:
The employee did have authorization to take the information home, however did not appropriately secure the information while it was in transit.

Resolution

On 01/06/12, the Privacy Officer (PO) interviewed the employee and updated the total number of Veterans affected. The box was examined by the PO and the employee stated the box was not tampered with. The PO completed the investigation on 01/13/12 and sent a letter to the employee's supervisor requesting appropriate corrective action and also recommended that the employee retake the Privacy and Security Awareness training and Rules of Behavior and the VA Privacy and HIPAA training.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000070506	Mishandled/ Misused Physical or Verbal Information	VBA St Petersburg, FL	1/9/2012	1/20/2012	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0540743	1/9/2012	INC000000191232	N/A	N/A	N/A	1	

Incident Summary

Veteran A received a letter meant for Veteran B. The letter contained Veteran B's name, address and SSN. A UPS shipping container was sent to Veteran A for document retrieval.

Incident Update

01/09/12:
Veteran B will be sent a letter offering credit protection services. The mis-mailed letter was returned to VA.

NOTE: There were a total of 109 Mis-Mailed incidents this reporting period. Because of repetition, the other 108 are not included in this report, but are included in the "Mis-Mailed Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

The Privacy Officer is unable to determine how this violation occurred. The credit protection letter was sent.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000070804	Missing/Stolen Equipment	VISN 06 Durham, NC	1/18/2012	2/1/2012	Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0542838	1/18/2012	INC000000193072	N/A	N/A	N/A	65	

Incident Summary

On 01/13/12, at approximately 4:30 PM, Doctor A noticed that his personal unencrypted MacBook Air laptop was missing from his office which was being gutted for new carpet placement. The laptop was last seen by Doctor B between 2:00 PM and 3:00 PM. Prior to gutting the room, staff members were asked to remove all valuable personal possessions or box them up for storage until the project is completed. Doctor A did not thoroughly remove/store his personal possessions. There is a chance that the laptop was boxed up and stored, but that cannot be determined until all the boxes are unpacked. There is no estimated completion date for that activity. Both Doctors A and B are in the habit of leaving their shared office door open during the normal tour of duty because they frequently go in and out to the Operating Room.

Approximately 3 years ago Doctor A transferred the contents of his old personal laptop to the MacBook Air. One of the folders included letters to VA patients. Shortly after the transfer, that folder was deleted. However, Doctor A is not sure that one or more letters weren't accidentally stored in another folder. It is unlikely that VA patient information is obviously visible to the casual observer, however, we cannot discount the possibility that some information remains.

The Service Chief, Chief of Staff, Director and Chief of VA Police were notified. If the laptop is found, Doctor A will contact the Information Security Officer. Recommendations for improved physical security were made to the Director.

Incident Update

01/20/12:
The Facility Police Service and the Information Security Officer (ISO) questioned the contractor who was installing the carpet. He did not see the MacBook Air and has voluntarily submitted a statement to the Police to that effect. The Facility has used this contractor for years without experiencing missing equipment issues. There are no cameras in this area. The Chief of Staff tasked an administrative staff member in the service with opening the boxes in which Doctor A stored his personal possessions for the renovation. She will begin searching the boxes today. Doctor A did not have a waiver to store information on his laptop. This facility has not authorized such storage since 2006. The ISO can only speculate as to why he wrote the patient letters on his personal laptop. Doctor A is on vacation and will return Monday. The ISO will get an answer to this question then. The Facility is investigating ways of recreating the group of patients to whom he sent letters.

01/23/12:
As of this update, the laptop has not been recovered. The Administrative Officer (AO) of the service has been through the office of the Doctor in question to search the packed boxes and was not able to find the laptop. With the likelihood that the laptop is not recovered, the AO is working on generating a list of patients that would have been seen by Doctor A and therefore could potentially be impacted. The Doctor will return on Monday morning and will be working to find the laptop and verify the list. Once complete, the list of potentially impacted patients will be given to the Privacy Officer.

01/24/12:
The ISO requested that Doctor A provide a plan with a due date for compilation of a list of patient names by tomorrow and copied the Chief of Staff and Associate Director.

01/25/12:
There were a total of 65 Veterans whose information (medical and full SSN) was on the MacBook Air laptop therefore 65 Veterans will receive a letter offering credit protection services.

Resolution

The letters were uploaded to the portal and mailed on 02/01/12. The Doctor has been notified not to store sensitive information on his laptop. The ISO requested improved physical security for the area with either use of the existing locks or installation of card readers or key pads for individual offices or the suite.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000070833	Mishandled/ Misused Physical or Verbal Information	VISN 23 Minneapolis, MN	1/19/2012		Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0543054	1/19/2012	INC000000193224	N/A	N/A	N/A	268	

Incident Summary

A Veteran reported receiving a clinic blood draw list attached to his blood draw appointment letter in the mail. The list included Veterans' names and full SSNs.

Incident Update

01/23/12:
The Veteran who received the list reported it and returned it the next day. Letters offering credit protection services will be sent to 268 Veterans due to full name and SSN being disclosed. It is not known who sent the list or where it was from, so all staff was reminded to check all documents before mailing them.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000070964	Missing/Stolen Equipment	VISN 17 San Antonio, TX	1/24/2012	1/30/2012	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0544002	1/24/2012	INC000000194014	N/A	N/A	N/A		

Incident Summary

While completing the annual IT equipment inventory, 1 laptop personal computer and 1 desktop computer were discovered missing and unaccounted for. Both of these computers were not formatted or configured with any VA information or images. The Director, Network Information Security Officer and the facility Police Service was notified. They are still investigating.

Incident Update

01/24/12:
No data breach has occurred. Neither the desktop computer nor the laptop was formatted, and neither had any VA information or data stored on it.

NOTE: There were a total of 5 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 4 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Resolution

IT has issued an Executive Summary for the Director's approval as well as a Report of Survey to say that there was no VA sensitive information on the missing devices.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000071062	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Hines, IL	1/25/2012		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0544486	1/25/2012	INC000000194380	N/A	N/A	N/A		1

Incident Summary

Patient A received a prescription intended for Patient B. Patient B's name and type of medication was compromised. Patient A reported the incident to the medical center and a replacement has been requested for Patient B. Great Lakes Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error. The CMOP employee(s) will be counseled and retrained in proper packing procedures.

Incident Update

01/26/12:
Veteran B will be sent a notification letter.

NOTE: There were a total of 4 Mis-Mailed CMOP incident out of 7,905,378 total packages (11,585,423 total prescriptions) mailed out for this reporting period. Because of repetition, the other 3 are not included in this report, but are included in the "Mis-Mailed CMOP Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000071237	Missing/Stolen Equipment	VISN 19 Salt Lake City, UT	1/31/2012		Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0545745	1/31/2012	INC000000195412	N/A	N/A	N/A		

Incident Summary

During the Bar Code Medication Administration (BCMA) laptop refresh, it was discovered that a BCMA laptop was missing. Information Resource Management (IRM) searched the department without success. Records show that a help desk ticket was opened on 11/07/11 and the laptop was last inventoried on 11/18/11. The BCMA laptop was not encrypted but did not contain sensitive information.

Incident Update

02/01/12:
No data breach occurred. The laptop contained no personally identifiable information (PII) or protected health information (PHI).

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000071428	Missing/Stolen Equipment	VISN 07 Montgomery, AL	2/3/2012		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0546621	2/3/2012	INC000000196176	N/A	N/A	N/A		

Incident Summary

Bio-Med was conducting annual preventive maintenance and noticed one of the laptops was missing. The laptop was not encrypted but the Innovian Draeger (clinical anesthesia information management system) software was password protected. There was no personally identifiable information (PII) or protected health information (PHI) stored on the laptop. It was last seen on 04/20/11 when it was inventoried.

Total number of Internal Un-encrypted E-mail Incidents	107
Total number of Mis-Handling Incidents	113
Total number of Mis-Mailed Incidents	109
Total number of Mis-Mailed CMOP Incidents	4
Total number of IT Equipment Inventory Incidents	5
Total number of Missing/Stolen PC Incidents	1
Total number of Missing/Stolen Laptop Incidents	5 (3 encrypted)
Total number of Lost BlackBerry Incidents	17
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	0