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

October 1 - November 4, 2012

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000081433	Missing/Stolen Material (Non-Equipment)	VISN 22 Las Vegas, NV	10/19/2012		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
VANSOC0582005	10/20/2012	INC000000242806	N/A	N/A	N/A	110	

Incident Summary

In August 2012, Dental staff performed patient record reviews. Upon completion they placed the records in a box, sealed and marked the box for Medical Records. In September four boxes were picked up from the Dental Office and taken to Medical Records by Mail Room employees. In the end of September 2012 Dental staff requested the boxes back, but only three boxes were returned. After searching the Dental Office and Medical Records spaces, the box was not located. This was approximately at the time clinics were moving into the new hospital. The box contained 110 patient Dental records.

Incident Update

10/22/12:
One hundred ten (110) Veterans will be sent letters offering credit protection services.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000081472	Missing/Stolen Equipment	VISN 18 Albuquerque, NM	10/22/2012	10/31/2012	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
VANSOC0582050	10/23/2012	INC000000243102	N/A	N/A	N/A		

Incident Summary

A computer was discovered missing at 08:00 AM on 10/22/12 by Employee A and reported to Police at 12:05 PM. She last saw the computer on Friday 10/19/12. The computer is a Dell Optic 755. The computer is not used for patient data. There is no risk. The computer tower was taken with the mouse and power strip. All data was entered into National Crime Information Center (NCIC). A review of the video is underway.

Incident Update

10/23/12:
The PC was set up as a MyHealtheVet kiosk, and was configured so that no data would be saved on the hard drive.

Resolution

After reviewing tape, the VA Police have no suspects. The video did not capture the suspect leaving the premises which means he or she departed through an exit without current coverage. No data breach occurred.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000081650	IT Equipment Inventory	VISN 12 Hines, IL	10/26/2012	11/5/2012	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
VANSOC0582240	10/26/2012	INC000000243944	N/A	N/A	N/A		

Incident Summary

During inventory of equipment on 10/25/12, it was discovered that a laptop was missing. The machine was last seen two months ago. The unit had been purchased for a Research project. The Hines Police will be contacted by the responsible service. The user of the PC has stated that to the best of his knowledge, there was no sensitive information stored on it.

Incident Update

10/26/12:
According to the laptop user, the laptop was not encrypted but the only items stored on the laptop were training presentations.

10/29/12:
The laptop was never directly on the VA network. The purpose of the laptop was to go with a projector used for lectures. They would load PowerPoint lectures via USB or disc, but when the use of these methods to save data became illegal, we switched to a IRM PC in a fixed location. The Information Security Officer's (ISO) last recall is that it was cable locked to a desk in the ISO's office, and when the desk was turned in, about February 2012, it was placed in a drawer in a code accessible room.

The Physician used it for a lecture earlier in the year, about the same time it was unlocked from the desk.

NOTE: There were a total of 3 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 2 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Resolution

A Police Report was filed. Police have no further information on this incident.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000081959	Mishandled/ Misused Electronic Information	VISN 15 Marion, IL	11/2/2012		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
VANSOC0582531	11/2/2012	INC000000245162	N/A	N/A	N/A		

Incident Summary

An email to a Summary Review Board team revealed that a VA Employee emailed a copy of the peer review letter that contained a patient's full name and last 4 digits of the SSN to the sender's personal Yahoo email address. The employee was advised that he should not email sensitive information to his personal email address and the employee revealed that he had the review attachments and several other items on the employee's home computer. The employee has been advised that this is inappropriate. This item remains open and under review.

Incident Update

11/05/12:
According to the Information Security Officer (ISO), due to the fact that the Employee is not at work today (11/05/12) it is not known at this time if the emails have been deleted from the Yahoo email account. The Employee's Supervisor is to contact the Employee to instruct him to delete the emails. At this time it is unknown if there are other such emails. The known email contains the name and partial SSN of a deceased patient. The ISO and Privacy Officer (PO) contacted Supervisor and instructed the Supervisor to make sure that the employee knows:

a. Sensitive email must not be sent unencrypted
b. Sensitive email must not be sent to personal email accounts
c. The unencrypted sensitive email must be deleted
d. The unencrypted personal email must be deleted.
e. The Supervisor is to make sure that Employee did not take any sensitive information home, if so it must be returned.

This issue remains open.

11/07/12:
The ISO is still working to get confirmation that files and emails deleted. The Employee is on administrative absence. The administrative action is being taken separately against the Employee.

11/13/2012:
Management is working on this issue. A letter is to go to the Employee that he needs to delete all VA data and to request redacted copies of any information the needs. Administrative action is pending.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000081965	Missing/Stolen Equipment	VISN 07 Birmingham, AL	11/2/2012		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
VANSOC0582538	11/2/2012	INC000000245174	N/A	N/A	N/A		

Incident Summary

On 11/02/12, at approximately 4:20 PM, the OIT Operations Manager notified the Information Security Officer (ISO) that a desktop PC was confirmed missing from room 1524-BH. An extensive search was conducted in the event the system was moved to another area/room within the Blue Clinic. Additional inquiries were made to last logon date and no logon was reported within the last 30 days. In addition, a secondary scan was made of Guardian Edge records with no current record of access. The system was last inventoried on: 05/01/12. This system was located in the rear of the area in a small cubical out of normal vision. It was discovered missing when additional staff was assigned to the work area. At this time it is unknown what data may have been stored on the device.

The Information Security Officer notified facility management, VA Police who have initiated an investigation, the Privacy Officer, and Network 7 ISO Supervisor.

Incident Update

11/05/12:
The desktop computer was not encrypted but it was password protected. It was just being placed into service and had just been loaded with the gold image and WIN 7. They were in the process of setting up a call center and this was one of 9 new PCs placed into the room for the call center. The machine was sitting in the call center room waiting for the staff to be moved into the area.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000080644	Mishandled/ Misused Electronic Information	VISN 01 Manchester, NH	10/1/2012	11/7/2012	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
VANSOC0581266	10/3/2012	INC000000239230	N/A	N/A	N/A	1	

Incident Summary

Veteran A received information on Veteran B in the mail from the Release of Information (ROI) Department. Veteran A returned the information to the Community Based Outpatient Clinic (CBOC), so that it could be returned to the correct Veteran. The information contained Veteran B's name, address, full SSN and diagnosis.

Incident Update

10/01/12:
Veteran B will be sent a letter offering credit protection services.

NOTE: There were a total of 149 Mis-Mailed incidents this reporting period. Because of repetition, the other 148 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 Supervisor addressed this with the employee. He was re-educated on the importance of protecting patient information and making sure to double check envelopes before mailing.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000080696	Mishandled/ Misused Physical or Verbal Information	VISN 07 Charleston, SC	10/1/2012	11/5/2012	High

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
VANSOC0581317	10/3/2012	INC000000239412	N/A	N/A	N/A	23	451

Incident Summary

A provider in Charleston South Carolina printed out a needs assessment for 474 patients. There were 23 patients with the full SSN and 451 with last four digits of the SSN and full name. They were printed to the library printer at the Cheyenne Wyoming VAMC.

Incident Update

10/02/12:
The documents were printed on 09/27/12 and not found until 09/28/12 at close of business. It was printed on a network printer in the facility library in an area open to the public. The papers were moved from the printer and placed on a desk near the printer and turned over. At this point, the facility does not know who removed them from the printer. The papers were locked up once they were found and on Monday were delivered to the Information Security Officer (ISO). The investigation continues on how the documents were printed from the Charleston VAMC to the Cheyenne VAMC.

10/09/12:
The person who found the item on the printer cannot be identified. Twenty-three letters offering credit protection services will be mailed to the patients who had their full SSNs potentially compromised. HIPAA letters of notification will be sent to the other 451 patients.

Resolution

The provider was placed on a Performance Improvement Plan (PIP). The provider chose to retire on 10/31/12.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000080850	Missing/Stolen Equipment	VISN 08 Bay Pines, FL	10/4/2012	10/4/2012	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
VANSOC0581461	10/8/2012	INC000000241097	N/A	N/A	N/A		

Incident Summary

There is a computer, monitor and keyboard missing from Medical Center Domiciliary Residential Library. The computer is for patient use only and is not connected to facility network. There is Steady State software used on the PC for user information protection.

Incident Update

10/04/12:
The PC was not on the VA network and was secured using Microsoft's Steady State and encryption.

Resolution

No data breach occurred.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000080897	Missing/Stolen Equipment	VISN 08 Tampa, FL	10/5/2012	10/5/2012	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
VANSOC0581502	10/5/2012	INC000000240270	N/A	N/A	N/A		

Incident Summary

A computer in storage was being turned in for disposal and the hard drive was missing. No sensitive data was stored on the hard drive since the computer was used for Animal Research. A VA Police Report was filed.

Incident Update

10/5/12:
The computer was stored in the Animal Research section of the hospital. It was only used for Animal Research and was 10 years old. It was last seen in 2004 in the OI&T section. The normal procedure is to remove the hard drive before the equipment is turned in. This appears to be a record keeping issue. No data breach occurred.

Resolution

10/05/12:
There was no personally identifiable information (PII) or protected health information (PHI) stored on the hard drive.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000081130	Missing/Stolen Equipment	VISN 23 Fargo, ND	10/12/2012	10/16/2012	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
VANSOC0581724	10/12/2012	INC000000241446	N/A	No	N/A		

Incident Summary

A PC used for paging was last inventoried by the previous telecommunications technician on 12/16/08. The equipment was purchased and received from Dell. The telecommunications technician remembers that this computer broke down and the prior technician used the computer as parts to repair other computers. This computer was only involved with pager setup and configurations and was never used as an administrative or medical PC. No patient data was ever present. An effort to locate the PC at other sites had no results.

Incident Update

10/15/12:
The server stored no personally identifiable information (PII) or protected health information (PHI) and was used for spare parts for other PCs.

Resolution

No breach occurred.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000081155	Mishandled/ Misused Physical or Verbal Information	VISN 01 Providence, RI	10/15/2012	10/16/2012	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
VANSOC0581746	10/15/2012	INC000000241611	N/A	N/A	N/A		1

Incident Summary

Veteran A received a prescription for Veteran B. The report states that the medication was handed out at the pharmacy window.

Incident Update

10/15/12:
Veteran B will be sent a HIPAA notification letter.

NOTE: There were a total of 149 Mis-Handling incidents this reporting period. Because of repetition, the other 148 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

Employee was educated on the importance of double checking scripts and Patient IDs prior to releasing meds.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000081209	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Hines, IL	10/15/2012	10/24/2012	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
VANSOC0581790	10/15/2012	INC000000241739	N/A	No	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

10/16/12:
Patient B will be sent a HIPAA letter of notification.

NOTE: There were a total of 4 Mis-Mailed CMOP incidents out of 7,701,938 total packages (10,787,258 total prescriptions) mailed out for this reporting period. Because of repetition, the other 3 is 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.

Resolution

The CMOP employee was counseled and retrained in proper packing procedures.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000081244	Missing/Stolen Equipment	VBA Portland, OR	10/16/2012	10/23/2012	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
VANSOC0581826	10/16/2012	INC000000241930	N/A	N/A	N/A		17

Incident Summary

The Portland Vocational Rehabilitation and Employment (VR&E) Officer received a phone call at 3:50 PM on 10/15/12 from Contractor A, Career Associates, stating that his residence was robbed. Contractor A asked the VR&E Officer to look at an email that he sent on 10/16/12 about the incident. Contractor A was working on Chapter 31 reports at his home, went to lunch, and at that time the house was robbed. Upon his return, Contractor A noticed his house was robbed and the laptop he was using to write Chapter 31 Veteran reports was stolen. It is not known at this time if the laptop and back-up drive were encrypted. A VA Police report is being filed, and will be sent to the facility when it becomes official.

Incident Update

10/17/12:
The laptop was privately owned equipment supplied by the Contractor. Seventeen (17) Veterans will be sent a general notification letter.

Resolution

The Contractors have been counseled by the VR&E Chief concerning the necessity of having updated email encryption on their computers. The Contractors are working with the Portland ISO to ensure their email encryption is initiated and utilized. The Portland ISO, Assistant Director, Portland Privacy Officer, and VR&E Management have all reached out to the Contractors to prevent any future security incidents from occurring. The Portland ISO will make quarterly contact with the contractors to discuss any security issues or concerns. The Contractors have indicated they will adhere to all VA regulations concerning Information Security and Privacy Awareness.

Total number of Internal Un-encrypted E-mail Incidents	133
Total number of Mis-Handling Incidents	149
Total number of Mis-Mailed Incidents	149
Total number of Mis-Mailed CMOP Incidents	4
Total number of IT Equipment Inventory Incidents	3
Total number of Missing/Stolen PC Incidents	6
Total number of Missing/Stolen Laptop Incidents	7 (6 encrypted)
Total number of Lost BlackBerry Incidents	15
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	1