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

February 4 - March 3, 2013

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000085414	Mishandled/ Misused Physical or Verbal Information	VISN 09 Nashville, TN	2/4/2013	2/7/2013	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
VANSOC0585872	2/4/2013	INC000000260400	N/A	N/A	N/A	1	

Incident Summary

Veteran A requested copies of his medical record to be mailed to his residence. Upon receiving his medical records in the mail, he also noticed that he received the medical records of Veteran B. Veteran A returned the medical records of Veteran B and they are now in the possession of the Privacy Officer (PO).

Incident Update

02/04/13:
Veteran B will be sent a letter offering credit protection services, as his full SSN and medical information were disclosed.

NOTE: There were a total of 97 Mis-Mailed incidents this reporting period. Because of repetition, the other 96 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 PO has completed credit protection letter and it was mailed on 02/07/13. This incident has already been referred to the Business Office for appropriate action concerning the employee involved. The PO confirmed the Business Office is in consultation with Human Resources for the appropriate action to be taken.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000085421	Mishandled/ Misused Physical or Verbal Information	VISN 01 West Haven, CT	2/4/2013	2/28/2013	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
VANSOC0585878	2/4/2013	INC000000260348	N/A	N/A	N/A	1	

Incident Summary

Veteran A was inadvertently given Veteran B's discharge diagnosis and medication name and dosage. The Physician realized the mishap and called Veteran A, who received the information. Veteran A was instructed to shred the information. The Chief Emergency Room Physician is calling Veteran A to see how the information was disposed of. The Privacy Officer (PO) informed the Physician that if the Veteran did not shred it ask the Veteran to forward the discharge summary back to the facility to the PO's attention.

Incident Update

02/04/13:
Veteran B will be sent a letter offering credit protection services as his full SSN and medical information was disclosed.

NOTE: There were a total of 106 Mis-Handled incidents this reporting period. Because of repetition, the other 105 are not included in this report, but are included in the "Mis-Handled 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 Physician was advised to be more careful.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000085842	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Leavenworth, KS	2/15/2013	2/28/2013	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
VANSOC0586273	2/15/2013	INC000000263143	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 Denver VA Medical Center (site 554) and a replacement has been requested for Patient B. Patient A returned Patient B's prescription bottle to Consolidated Mail Outpatient Pharmacy (CMOP) for destruction. Leavenworth 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

02/13/13:
Patient B will be sent a notification letter.

NOTE: There were a total of 6 Mis-Mailed CMOP incidents out of 6,314,952 total packages (9,448,375 total prescriptions) mailed out for this reporting period. Because of repetition, the other 5 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.

Resolution

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

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000085986	Missing/Stolen Equipment	VISN 16 Alexandria, LA	2/21/2013		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
VANSOC0586419	2/21/2013	INC000000264026	N/A	N/A	N/A		

Incident Summary

A VA computer system was removed from the facility. The system was a desktop and unencrypted. The CPU, monitor, keyboard, mouse, power managements system, and network cables were all removed. There was no known personally identifiable information (PII) or protected health information (PHI) on local hard drive. The computer was last seen on Tuesday, 02/19/13 after 3:00 PM. It was noticed missing on Wednesday morning, however, it was assumed (since the area was cleaned) that OIT had removed the system. OIT reported that no one removed the computer. The investigation continues.

Incident Update

02/25/13:
It is not known when the computer was last connected to the network, however it was last logged onto on 02/19/13 by a physician. The intended use was for staff to access CPRS. There are no cameras in the area which may show who took the computer.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000086132	Missing/Stolen Equipment	VACO Field Program Office Atlanta, GA	2/26/2013	2/28/2013	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
VANSOC0586555	2/26/2013	INC000000265015	N/A	N/A	N/A		

Incident Summary

During a recent inventory inspection, two laptops and two desktops were discovered missing from the designated IT storage room. These devices were never connected to the network and were not issued to users. At no time was Personally Identifiable Information (PII), Personal Health Information (PHI) or Federal Tax Information stored on the laptops. Per Big Fix software, none of the devices were connected to the network.

Incident Update

02/26/13:
No data breach has occurred. The devices had never been on the VA network, never contained PII or PHI, and were never issued to users.

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

The facility added security cameras and updated authorized access to the location. Each employee who pulls equipment must now document the action.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000086142	Missing/Stolen Equipment	VBA Philadelphia, PA	2/26/2013	2/28/2013	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
VANSOC0586568	2/26/2013	INC000000265069	N/A	N/A	N/A		

Incident Summary

On Tuesday, 02/26/13, several National Pension Call Center employees at the Philadelphia Regional Office, reported that they came in and found things in a disarray and a monitor and CPU were missing. The make and model of the computer was a Dell 990, which was encrypted. This has been reported to management and Federal Protective Service, who was on the scene. Surveillance pictures from an interior camera show an unidentified, non-VA employee, who pried his way in, through an access controlled door. Additionally, a Personal Identity Verification (PIV) card was stolen and it has been disabled.

Incident Update

02/28/13:
The computer was encrypted, and no paper personally identifiable information (PII) appears to have been removed or is missing.

Resolution

No breach occurred.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000086171	Missing/Stolen Equipment	Corporate Regional Readiness Center (CRRC) Martinsburg, WV	2/27/2013	3/11/2013	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
VANSOC0586594	2/27/2013	INC000000265239	N/A	N/A	N/A		

Incident Summary

A VA employee reported that his VA laptop has been stolen from his rental car while on VA travel. The laptop is encrypted. A San Francisco Police Report has been filed.

Incident Update

02/27/13:
Per the Information Security Officer (ISO), no personally identifiable information (PII) or protected health information (PHI) was stored on the laptop. The laptop was last on the VA network on 02/26/13 at 10:00 AM. It was last seen on 02/26/13 at 7:30 PM. It was in a back pack in the back of the rental car but the laptop was not visible. The employee was not on duty at 7:30 PM. The VA USB broadband card was also taken.

Additional items, including the employee's personal laptop, iPad, camera, and Bose headphones, were also taken.

03/04/13:
The VA inventory folks have completed a Report of Survey. The risk to the VA appears to be minimal given the fact there was no VA sensitive data on the device and it was encrypted.

03/11/13:
The Police Report and VA Report of Survey have been completed for this stolen device. The device was encrypted and contained no VA Sensitive Data.

Resolution

The PO has no additional information. The laptop was encrypted. No data breach occurred.

Total number of Internal Un-encrypted E-mail Incidents	89
Total number of Mis-Handling Incidents	106
Total number of Mis-Mailed Incidents	97
Total number of Mis-Mailed CMOP Incidents	6
Total number of IT Equipment Inventory Incidents	3
Total number of Missing/Stolen PC Incidents	2
Total number of Missing/Stolen Laptop Incidents	7 (6 encrypted)
Total number of Lost BlackBerry Incidents	18
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	1