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

June 4 - July 1, 2012

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000076325	Mishandled/ Misused Physical or Verbal Information	VISN 07 Montgomery, AL	6/4/2012	6/25/2012	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
VANSOC0571687	6/4/2012	INC000000217737	N/A	N/A	N/A	1	

Incident Summary

Veteran A called the Central Alabama Veterans Health Care System (CAVHCS) and the Veterans Integrated Service Network (VISN) to report he received a letter in the mail containing Veteran B's name and SSN. The Privacy Officer (PO) has contacted Veteran A to retrieve the mismailed letter.

Incident Update

06/05/12:
Veteran B will be sent a letter offering credit protection services.

NOTE: There were a total of 104 Mis-Mailed incidents this reporting period. Because of repetition, the other 103 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 employee was retrained on the importance of double-checking documents to ensure the correct patient information is present before mailing the documents. If needed, the employee can use a brief checklist to ensure accuracy.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000076379	Mishandled/ Misused Physical or Verbal Information	VISN 17 Temple, TX	6/5/2012		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
VANSOC0571871	6/5/2012	INC000000218065	N/A	N/A	N/A		389

Incident Summary

A Veteran patient reported that while walking through the facility, she came upon a stack of papers that was unattended. The paperwork was determined to be an inpatient list containing the full name, partial SSN, admission date, and ward location of 389 Veterans. The Veteran immediately located the nearest information desk and returned custody of the information to a staff member. The information was never outside the confines of the facility.

Incident Update

06/10/12:
The 14 page inpatient list was located in a major hallway on a ledge that contained free reading materials (novels, magazines). The list was printed at 7:04 AM and was found at 1:50 PM. There is no way of definitely knowing when or how long the list was left there. This area is one of the most traveled areas in the facility as it is the main entrance from the valet parking area and used to transition from the inpatient to the outpatient areas of the facility. There are video cameras in the area however they were not focused on that particular area of the hallway.

06/13/12:
Per the decision made by the national VA Data Breach Core Team, the 389 Veterans will receive notification letters due to their full names and Protected Health Information (PHI) being exposed in a major hallway for an unknown length of time.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000076384	Mishandled/ Misused Physical or Verbal Information	VISN 08 Tampa, FL	6/6/2012	6/13/2012	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
VANSOC0571902	6/6/2012	INC000000218160	N/A	N/A	N/A	1	

Incident Summary

Veteran A was given Veteran B's discharge instructions upon discharge from Urgent Care. The documents contained Veteran B's name, full SSN and discharge instructions.

Incident Update

06/04/12:
Veteran B will be sent a letter offering credit protection services.

NOTE: There were a total of 112 Mis-Handling incidents this reporting period. Because of repetition, the other 111 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 responsible employee was required to re-take the appropriate training modules. The employee's Supervisor was instructed to consult with Human Resources (HR) to determine if any disciplinary action is deemed necessary.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000076418	Missing/Stolen Equipment	VISN 11 Indianapolis, IN	6/6/2012	6/8/2012	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
VANSOC0572001	6/6/2012	INC000000218335	N/A	N/A	N/A		

Incident Summary

After a recent equipment inventory, Logistics Service reported a VA PC missing. The PC was never connected to the VA network and was utilized by Engineering Service to control environmental control systems. The PC was purchased in 1998 and never contained VA sensitive information.

This issue appears to be related to the inventory turn-in process. The PC was taken out of service and last inventoried in July 2011 at the location where hard drives are sanitized, so the hard drive was most likely destroyed, and then the PC was sent to the warehouse to be scrapped. However, documentation associated with the PC turn-in was not completed.

Incident Update

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

Staff members involved with the turn-in of PCs has been re-trained on completing of all required documentation. The Logistics Service has completed a Report of Survey (RoS) to document this PC as lost.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000076463	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Murfreesboro, TN	6/7/2012	7/2/2012	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
VANSOC0572177	6/7/2012	INC000000218469	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. Murfreesboro 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

06/07/12:
One patient will be sent a letter of notification.

NOTE: There were a total of 9 Mis-Mailed CMOP incidents out of 6,305,975 total packages (9,385,475 total prescriptions) mailed out for this reporting period. Because of repetition, the other 8 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 was counseled and retrained in proper packing procedures.

Total number of Internal Un-encrypted E-mail Incidents	111
Total number of Mis-Handling Incidents	112
Total number of Mis-Mailed Incidents	104
Total number of Mis-Mailed CMOP Incidents	9
Total number of IT Equipment Inventory Incidents	3
Total number of Missing/Stolen PC Incidents	5
Total number of Missing/Stolen Laptop Incidents	13 (13 encrypted)
Total number of Lost BlackBerry Incidents	20
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	0