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

September 3 - 30, 2012

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000079838	Mishandled/ Misused Physical or Verbal Information	VISN 04 Lebanon, PA	9/5/2012	9/19/2012	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
VANSOC0580460	9/5/2012	INC000000234488	N/A	N/A	N/A	1	

Incident Summary

When Veteran A was checking out in the clinic area, he received Veteran B's appointment information showing full name, full social security number and appointment data information. Veteran A mailed the paperwork to the Privacy Officer (PO). The PO received the paperwork today and reported the incident.

Incident Update

09/05/12:
Veteran B will receive a letter offering credit protection services.

NOTE: There were a total of 102 Mis-Handling incidents this reporting period. Because of repetition, the other 101 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

Staff members were reminded on the importance of safeguarding patient identifiable information.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000079906	Missing/Stolen Equipment	VISN 18 Phoenix, AZ	9/6/2012		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
VANSOC0581344	9/7/2012	INC000000234934	N/A	N/A	N/A		

Incident Summary

The Information Security Officer (ISO) was notified by Research that one of two sponsor provided laptops has been out of VA's control since July 2012. Apparently, a former Without Compensation (WOC) Research employee possessed the unaccounted for HP Netbook laptop. The former WOC Research employee was a member of the study team. The Research office was unaware that the sponsor had provided two laptops for the study. Therefore, Research did not have it listed among their assets nor were they able to request its status during the former employee's station clearance. Recently, the laptop was handed over to a current Research WOC employee. It is unclear when the hand off took place and what motivated the former employee to hand it off to the current Research WOC. However, the current WOC will be providing the laptop to Research today. A chain of custody form will be filled out upon Research's receipt of the HP Netbook. The local Incident Response team has met and our investigation is still ongoing.

Incident Update

09/10/12:
The non-VA laptop was not encrypted because the laptop was provided by New York University who was the sponsor of the study. It is unknown at this time if any VA data is on the laptop. According to the current WOC and Acting Chief of Research, the ISO was advised that the laptop was not connected for the purpose of the study. The laptop is now in custody of the VA and the ISO is still investigating whether there was/is any VA data on the laptop.

09/11/12:
The Facility has requested that the VA NSOC look at it to do the forensics on laptop.

10/09/12:
The NSOC received the hard drive last week and a forensic image of it was taken. This case is in the NSOC queue right now and analysis will begin once other active cases are completed.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000080000	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Leavenworth, KS	9/10/2012	10/2/2012	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
VANSOC0580628	9/12/2012	INC000000235734	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. Leavenworth 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

09/11/12:
Patient B will be sent a notification letter.

NOTE: There were a total of 2 Mis-Mailed CMOP incidents out of 6,157,152 total packages (9,223,894 total prescriptions) mailed out for this reporting period. Because of repetition, the other 1 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
SPE000000080103	Missing/Stolen Equipment	VISN 08 Gainesville, FL	9/13/2012	9/19/2012	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
VANSOC0580734	9/14/2012	INC000000236159	N/A	N/A	N/A		

Incident Summary

Due to a previous loss of an unencrypted laptop by the Research Service, the Deputy Director ordered a top to bottom inventory of Research laptops. During the inventory, 2 were discovered missing. Both were not encrypted and were used in the Animal Research lab.

Incident Update

09/14/12:
The laptops were not able to connect to the VA network and did not contain any patient or employee information since they were used for Animal Research.

NOTE: There were a total of 7 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 6 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Resolution

No breach occurred.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000080452	Mishandled/ Misused Physical or Verbal Information	VBA Boise, ID	9/24/2012		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
VANSOC0581080	9/26/2012	NC000000238098	N/A	N/A	N/A	2	

Incident Summary

A Veteran received his notification letter along with two other Veteran's letters through the mail. The letters contained the two Veterans' names, addresses and full SSNs

Incident Update

09/24/12:
The other two Veterans will be sent offers for credit protection services, as their full SSN was disclosed.

NOTE: There were a total of 77 Mis-Mailed incidents this reporting period. Because of repetition, the other 73 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.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000080509	Mishandled/ Misused Physical or Verbal Information	VISN 08 San Juan, PR	9/25/2012		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
VANSOC0581139	9/26/2012	INC000000238375	N/A	N/A	N/A	84	

Incident Summary

During a routine inspection today at 11:30 AM at the Neurology Lab for some construction work that is being performed, the Medical Service Chief entered room 1F184 Neurology where EEG technicians work and identified in unlocked drawers and desks lots of documents with the name and social security numbers of about 296 patients. The documents identified were old Sleep Studies, some dating back to 2011, appointment lists and hand written documents with lists of patients and SSNs. All these documents were seized and are under custody. The door of the EEG room was locked at the time the Privacy Officer (PO) entered but the documents were unsecured. During the inspection, the Medical Service Chief was accompanied by the Service Administrative Officer, Automated Data Processing Application Coordinator (ADPAC), the Acting Chief of Neurology, and an LPN assigned to the area.

Incident Update

10/01/12:
The room is typically locked when not in use, and most of the information was out of sight (in cabinets and drawers), however, 84 individuals information was out in plain sight. These 84 individuals will receive letters offering credit protection services due to full name and full SSN being exposed.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000080634	Mishandled/ Misused Physical or Verbal Information	VISN 20 Seattle, WA	9/28/2012		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
VANSOC0581256	9/29/2012	INC000000239072	N/A	N/A	N/A	71	

Incident Summary

A Human Resource (HR) employee discovered five pieces of paper in a shrub near one of the buildings at the VA Puget Sound American Lake Hospital. It was an "Inpatient Religious Affiliations Listing by Ward," which is typically used by VA Chaplains when conducting their daily rounds. The listing contains the names of seventy-one (71) inpatients, their race, age, DOB, SSN, admission date/time, diagnoses, religion and room number.

Incident Update

10/01/12:
Seventy-one (71) patients will receive a letter offering credit protection services.

Total number of Internal Un-encrypted E-mail Incidents	105
Total number of Mis-Handling Incidents	102
Total number of Mis-Mailed Incidents	77
Total number of Mis-Mailed CMOP Incidents	2
Total number of IT Equipment Inventory Incidents	4
Total number of Missing/Stolen PC Incidents	2
Total number of Missing/Stolen Laptop Incidents	7 (6 encrypted)
Total number of Lost BlackBerry Incidents	21
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	1