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

July 2 - August 5, 2012

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000077421	Mishandled/ Misused Physical or Verbal Information	VBA Sioux Falls, SD	7/2/2012	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
VANSOC0575110	7/2/2012	INC000000222926	N/A	N/A	N/A	1	

Incident Summary

Veteran A was inadvertently mailed Veteran B's information, including Veteran B's full name, full SSN, mailing address and date of birth.

Incident Update

07/02/12:
Veteran B will be sent a letter offering credit protection services.

NOTE: There were a total of 125 Mis-Mailed incidents this reporting period. Because of repetition, the other 124 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 credit monitoring letter has been mailed out to the Veteran. Management has addressed the issue with the responsible employee.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000077427	Mishandled/ Misused Physical or Verbal Information	VISN 15 Kansas City, MO	7/2/2012	8/13/2012	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
VANSOC0575125	7/2/2012	INC000000222962	N/A	N/A	N/A	1	

Incident Summary

Veteran A called the Privacy Officer (PO) at 10:15 AM to report that, upon his arrival home after his Emergency Department visit on Saturday, 06/30/12, he realized that he had been given Veteran B's paperwork. Veteran A stated that due to medication given to him, he is unable to provide a description of the individual who handed him the paperwork. Additionally because of his problems with reading, he is unable to provide details about the content of the paperwork he received. He was agreeable to return the paperwork to the PO via the mail. Veteran A expressed some concern about whether or not his information was given to another Veteran since another Veteran's information was given to him. He did state the document contained the name, SSN and medications of Veteran B.

Incident Update

07/02/12:
Veteran B will be sent a letter offering 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 staff Involved was counseled. The employee was required to take the refresher Education and Awareness Training.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000077437	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Murfreesboro, TN	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
VANSOC0575161	7/2/2012	INC000000223002	N/A	N/A	N/A		1

Incident Summary

Patient A received a Consolidated Mail Outpatient Pharmacy (CMOP) prescription package intended for Patient B. Patient B's name, address, and type of medication was compromised. Patient A reported the incident to the medical center and a replacement has been requested for Patient B. Murfreesboro Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a mail consolidator error. The packing labels were misapplied to the package. The mail consolidator has been notified of the error and will take corrective action.

Incident Update

07/02/12:
Veteran B will be sent a notification letter.

NOTE: There were a total of 5 Mis-Mailed CMOP incidents out of 7,593,128 total packages (11,458,576 total prescriptions) mailed out for this reporting period. Because of repetition, the other 4 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
SPE000000077524	Missing/Stolen Equipment	VISN 07 Montgomery, AL	7/5/2012	8/14/2012	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
VANSOC0575461	7/5/2012	INC000000223526	N/A	N/A	N/A		

Incident Summary

Central Alabama Veterans Health Care System (Montgomery Campus) conducted its OI&T Annual Inventory. The following equipment could not be located: 10 CPUs, 2 laptop computers, 1 BlackBerry, and 4 servers. The missing equipment did not contain any personally identifiable information (PII) or protected health information (PHI).

Incident Update

07/09/12:
The laptops are encrypted. Two of the servers have been found.

0713/12:
Several items have been located. As of this date, 6 computer PCs, 2 laptop computers, and 4 BlackBerry smart phones are still missing:

NOTE: There were a total of 4 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 3 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Resolution

The Report of Survey has been completed for the missing equipment.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000077664	Missing/Stolen Equipment	VISN 08 Miami, FL	7/10/2012		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
VANSOC0575882	7/10/2012	INC000000224370	7/10/2012	Yes	Pending		

Incident Summary

A VA employee went to the Research Conference Room to help with a presentation and there was no computer there. The employee told Information Resource Management Service (IRMS) and they advised that they didn't have the computer. So a report was made to the VA Police and the Information Security Officer (ISO).

Incident Update

07/11/12:
Per the ISO, this was a desktop computer in the conference room and did not store personally identifiable information (PII) or protected health information (PHI).

08/14/12:
The ISO is waiting for the VA Police Report.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000077988	Missing/Stolen Equipment	VISN 03 East Orange, NJ	7/18/2012		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
VANSOC0576819	7/18/2012	INC000000225782	N/A	N/A	N/A		

Incident Summary

It was reported yesterday by a user that 2 contractor tablet PCs were stolen from the East Orange Campus. According to the employees, there was no patient data stored on these devices. They were utilized only for survey purposes.

Incident Update

07/18/12:
The tablet PCs were not encrypted, however they did not contain any personally identifiable information (PII) or protected health information (PHI) and were not connected to the VA network. They were used to take anonymous customer satisfaction surveys as to the satisfaction of the care they received while at the facility.

07/19/12:
The Privacy Officer (PO) confirmed that the tablet PCs were used to take customer satisfaction surveys. They were equipped with mobile broad band cards allowing them access to the internet. Upon discharge, patients were asked questions such as "was the color of the room pleasing?" The tablet was used to access a web based application to enter the answers to these questions. The room and bed number were entered but no other identifying information was entered. No data was stored on the tablets.

07/20/12:
After Speaking with the President of TruthPoint Company, the Information Security Officer (ISO) was informed that VA purchased the tablets from TruthPoint on a VA VISN contract dating back to 2010. The ISO inspected the remaining tablets and there are no government markings on these tablets to indicate government ownership. The President of TruthPoint also indicated that there is a built-in encryption from TruthPoint that encrypts the answers to the survey when stored on the tablet and only TruthPoint has an encryption key to open and view the data. In addition, when survey results are transmitted to TruthPoint via a MiFi device (No VA network connection) for processing, files on the tablet are automatically erased.

According to the President, the last time both tablets transmitted data to the company was on 07/16/12 at or about 6:00 PM. The units in question were reported missing by NJ staff the morning of 07/17/12. Based on these facts, it is a strong possibility that at the time of the actual theft, these units contained none of the normally collected survey information. The survey information collected by staff at NJ is deemed not sensitive (no PII or PHI).

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000078049	Missing/Stolen Material (Non-Equipment)	VISN 10 Dayton, OH	7/19/2012		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
VANSOC0576977	7/19/2012	INC000000226051	N/A	N/A	N/A		

Incident Summary

It was reported to the Privacy Officer (PO) that a log book is missing from a service. It contains at least the patients' names and last four digits of their SSNs. At this point, no additional information is available. The PO is investigating.

Incident Update

07/19/12:
The log book was used in Surgery Service to track patients who developed complications after receiving anesthesia. It is not known how many Veterans are identified in the log. The PO is investigating.

07/24/12:
Information received from the staff person and chief is that an unknown number of patients' information is at risk. The entire Anesthesia (Surgery) staff was questioned as to the whereabouts of the log book which is the Anesthesia Morbidity & Mortality Book. The log book contains patients' names, procedures, last four digits of the SSN, and complications. It was reported to VA Police to investigate.

08/03/12:
The log book remains missing and cannot be located. In order to minimize risk and ensure appropriate safeguards are used to maintain security, a communication will be sent to the service chiefs advising that "the use of paper log books is prohibited unless special approval is granted in writing by the Medical Center Director or designee." An extensive review of work areas is being conducted, to retrieve any log books.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000078418	Mishandled/ Misused Physical or Verbal Information	VBA Muskogee, OK	7/26/2012		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
VANSOC0577870	7/26/2012	INC000000227448	N/A	N/A	N/A	51	

Incident Summary

Veteran A received benefits for 51 other Veterans in his account. He used a form from the internet that caused a college's account to be deposited into his account. The bank then sent Veteran A, a list of the Veterans whose checks went into his account. The bank called Veteran A and told him to destroy the list.

Incident Update

07/27/12:
Veteran A got access to a VA Form 22-8794a online. This form is used to change banking information for schools. He asked and received from Temple College their Federal ID and their Facility Code. He listed his name as the person making the change and used his personal banking information. It did not appear to be a fraudulent attempt to obtain the school funds. He really thought he was changing his banking info.

This information made it to the local Education Liaison Representative (ELR) who changed the Temple College banking information. For March and April 2012 payments for other Veterans went to Veteran A's bank account. The total amount was $121,279.51. The Veteran called VA and reported this happening. We have listened to the recording of the call. The call agent who answered the phone advised him that those were probably not VA payments since they did not show up as being issued on his payment history screen. They would not show since they belonged to other Veterans. Temple College had already contacted another ELR who made a banking change to direct funds to the proper school account.

VA issued reclamation requests for all 162 deposits that had been made to Veteran A's account. We received $99,394.51 back. This left a balance of $21,885.00 that could not be recouped. The facility discussed this with the Veteran who advised that he had disposed of six checks he received from VA since he knew the money was coming in by Direct Deposit. We have placed stop payments on these outstanding checks. When these funds are returned, they will be deducted from his debt.

This was picked up by a TV station in Temple, TX, and made their news. When we investigated, we asked for the banking information and addendum information on the deposits going to the Veteran's account. When they sent copies to us, they also sent copies to Veteran A. The addendum information has SSNs and names of 51 Veterans whose payments were deposited to Veteran A's account.

The credit union where Veteran A's account was located has offered to issue credit monitoring to those 51 Veterans, and they will need names and addresses to go with the SSNs. The VBA Muskogee facility would have to provide names, addresses, and SSNs to the credit union for this to happen, which isn't a permissible disclosure.

07/31/12:
The Data Breach Core Team (DBCT) met and discussed this. It was determined by the Office of General Counsel (OGC) and the DBCT that VA should provide credit protection services and clearly state in the offer that the data breach was caused by the credit union but VA is providing the credit protection services to the Veterans.

Resolution

VA did NOT cause this incident but VA sent a letter that offered credit protection services to all 51 Veterans.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000078723	Missing/Stolen Material (Non-Equipment)	VISN 05 Martinsburg, WV	8/3/2012		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
VANSOC0578697	8/3/2012	INC000000228864	N/A	N/A	N/A		268

Incident Summary

VA Public Affairs Employee A was working with a Veteran on MyHealtheVet (MHV) registration at a reception desk in the corridor. There was a patient appointment list on the credenza behind the reception desk on a clipboard which Employee B had been using prior to leaving for the day. Employee A was using the same desk to register MHV patients. Employee A started getting ready to leave for the day and realized that the appointment list was not on the clipboard. Employee A texted Employee B to find out if the appointment list had been shredded but was told to check on the credenza behind the desk and it was not there. Employee A conducted a thorough search and checked with other staff in the area in case someone had picked it up but nobody had seen the list and it was reported missing.

There were 268 Veteran patients listed on the appointment list which included each Veteran's name, clinic name, time of the clinic appointment and the last four digits of the SSN.

Incident Update

08/03/12:
The 268 Veterans will receive a HIPAA notification letter.

Total number of Internal Un-encrypted E-mail Incidents	136
Total number of Mis-Handling Incidents	113
Total number of Mis-Mailed Incidents	125
Total number of Mis-Mailed CMOP Incidents	5
Total number of IT Equipment Inventory Incidents	4
Total number of Missing/Stolen PC Incidents	6
Total number of Missing/Stolen Laptop Incidents	5 (4 encrypted)
Total number of Lost BlackBerry Incidents	26
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	0