

Department of Veterans Affairs



**Monthly Report to Congress
On Data Incidents**



October 2010

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category	
SPE000000051170	Privacy	VISN 16 Fayetteville, AR	10/4/2010	10/6/2010		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
VANSOC0396495	10/4/2010	INC000000115013	N/A	N/A	N/A	0	1
Incident Summary							
Veteran A contacted the pharmacy to say that he received Veteran B's medication paperwork with Veteran A's medication in the mail. Veteran B's full name and address were disclosed.							
Incident Update							
10/04/10: Veteran B will receive a notification letter. The SSN was not disclosed.							
NOTE: There were a total of 115 Mis-Mailed incidents this reporting period. Because of repetition, the other 114 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 notification letter was sent.							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000052007	Privacy	VISN 16 Fayetteville, AR	10/5/2010	10/27/2010		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
VANSOC0397285	10/5/2010	INC000000115298	N/A	N/A	N/A	0	1

Incident Summary

Veteran A came to the pharmacy window to pickup his medication. Veteran A came back a second time to pick up additional medication and was mistakenly given Veteran B's medication. Veteran A will return Veteran B's medication on his return appointment on 11/03/10.

Incident Update

10/06/10:
Veteran B will receive a letter of notification.

NOTE: There were a total of 79 Mis-Handling incidents this reporting period. Because of repetition, the other 78 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 notification letter was sent on 10/14/10.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category	
SPE000000052908	Missing/Stolen VA Resources	VBA Huntington, WV	10/8/2010			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
VANSOC0399156	10/8/2010	INC000000115909	N/A	N/A	N/A		

Incident Summary

A VA job lab workstation is missing. This workstation was assigned to the Huntington Regional Office Vocational Rehabilitation and Employment (VR&E), which is responsible for tracking these assets when assigned to them. Multiple manual inventories were performed by IT personnel in the attempt to locate the computer. It is believed by IT after talking to VR&E that this computer was not accessible and could not be utilized by VR&E or Veterans when it was available. This is being reported because all possible options have been exhausted trying to locate the computer.

Incident Update

10/08/10:

According to the ISO, the computer was never on the VA network and no PHI/PII was on the computer. The computer was last seen in the VR&E storage closet.

11/03/10:

Historically, VR&E was responsible for tracking job lab computer locations and assignments so the job lab computers were never included in the IT inventories. Currently four of five job lab computers are accounted for and have been added to the IT inventory list. According to the information available, IT has no record of the missing workstation regarding purchase, disposal, check in/out, software image or annual inventory. A manual search for the computer, including work at home employees and employees who have relocated to other VA offices, did not turn up the missing computer. A Report of Survey has been done.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category	
SPE000000052913	Privacy	VBA Nashville, TN	10/8/2010			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
VANSOC0399339	10/8/2010	INC000000115963	N/A	N/A	N/A	240	0
<p>Incident Summary A Regional Office (RO) guard found an unencrypted thumb drive inside the facility doors. The RO guard took the drive home to investigate and identified Veterans' information on the device. RO guard contacted the RO the next morning and returned the thumb drive to VA custody. The thumb drive belonged to a VA staff member. Investigation is ongoing. Leadership and Privacy Officer were notified.</p>							
<p>Incident Update 10/12/10: According to the ISO, the personal thumb drive had fiduciary information for approximately 186 Veterans and/or beneficiaries. Their full names, SSNs, DOBs, mailing addresses, medical data (health information), and other financial information was included. The thumb drive was the personal property of the employee. The employee was not authorized to maintain VA sensitive information on a thumb drive. The employee failed to follow VA policies and procedures. A statement provided by the RO guard indicates the information was shared with the guard's spouse who "maintains a high security clearance thru Department of Justice and DEA." The guard's spouse identified the information on the thumb drive as VA sensitive information and the thumb drive was turned in VA custody the next morning. The thumb drive was unattended/lost for approximately 16 plus hours and the contents were seen by unauthorized persons. The 186 Veterans will receive a letter offering credit protection services.</p> 10/22/10: After further investigation, the total count of unique Veterans requiring credit protection services is 240 individuals.							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category	
SPE000000053029	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Charleston, SC	10/12/2010	11/4/2010		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
VANSOC0400926	10/12/2010	INC000000116297	N/A	N/A	N/A	0	1
Incident Summary							
<p>Patient A received one supply item from Medline Industries intended for Patient B. This incident was reported to the Richmond VAMC (station 652) by Patient A and the Richmond VAMC reported to Charleston CMOP on October 8, 2010. The supply item and paperwork contained Patient B's name and supply item name. No SSN data was compromised. Patient A contacted the Richmond VAMC to report the error. The Richmond VAMC contacted Patient B's medical center to resend. Investigation reveals that Patient A and Patient B's orders were processed at Medline. The packaging error has been reported to Medline for investigation and corrective actions.</p>							
Incident Update							
<p>10/13/10: Veteran B will receive a notification letter.</p> <p>NOTE: There were a total of 10 Mis-Mailed CMOP incidents out of 5,794,258 total packages (8,505,664 total prescriptions) mailed out for this reporting period. Because of repetition, the other 9 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.</p>							
Resolution							
<p>The notification letter was mailed on 11/01/10.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category	
SPE000000053176	Missing/Stolen Material (Non-Equipment)	VISN 16 Oklahoma City, OK	10/15/2010			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
VANSOC0402517	10/15/2010	INC000000116982	N/A	N/A	N/A	0	1950
<p>Incident Summary</p> <p>On 10/15/10, an employee reported that multiple pages from an Oklahoma VAMC pulmonary laboratory log book are missing. The log book pages contained patient names and partial Social Security number along with lab test abbreviations. Preliminary investigation indicates that this involved a personnel issue and that the documents were likely shredded but this has not yet been confirmed. The pages missing from the lab log book could contain up to 1,950 Veterans' names, appointment times and dates, last 4 of the SSNs, mod/unit, requesting physicians, tests, and lab numbers from 01/01/10 until 10/08/10. This issue is still under investigation.</p>							
<p>Incident Update</p> <p>10/19/10: Since there is no proof that the log book pages were shredded, 1,950 Veterans will receive a notification letter. Due to the number of Veterans affected this will require a public notice and HITECH submission.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category	
SPE000000053558	Missing/Stolen Material (Non-Equipment)	VISN 07 Montgomery, AL	10/21/2010			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
VANSOC0405616	10/21/2010	INC000000118068	N/A	N/A	N/A		

Incident Summary

A Logistics Inventory Management Specialist was conducting a wall to wall inventory when she noticed that a workstation and monitor was missing. Police and Security were called and a Uniform Offense Report was submitted.

Incident Update

10/23/10:

The ISO states the workstation was not encrypted. According to the Chief of Nutrition the workstation interfaced with the Food and Nutrition Cook/Chill System. The workstation was never installed, and it was still in the box in Food and Nutrition area. This area in Food and Nutrition has been under construction for some time. The PC was inventoried in the box in February 2010. Logistic Service was conducting their 6 month inventory and found that a box was missing. The PC belongs to Food and Nutrition Service. The PC/monitor was never taken out of the Dell Package. No PII/PHI was on the PC.

NOTE: There were a total of 2 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 1 is not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category	
SPE000000053779	Mishandled/ Misused Physical or Verbal Information	VISN 03 Bronx, NY	10/25/2010			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
VANSOC0406825	10/25/2010	INC000000118603	N/A	N/A	N/A	146	
<p>Incident Summary</p> <p>The Education Department was moving from one storage area to another and a box containing information pertaining to employees who took the Cardiopulmonary Resuscitation (CPR) test was left in the open. The location was accessible by employees as well as volunteers. Privacy information included employee's names and social security numbers.</p>							
<p>Incident Update</p> <p>10/26/10: One hundred and forty six (146) employees will receive a letter offering credit protection services.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category	
SPE000000053804	Mishandled/ Misused Physical or Verbal Information	VISN 21 Honolulu, HI	10/25/2010	11/4/2010		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
VANSOC0407118	10/25/2010	INC000000118724	N/A	N/A	N/A	180	
Incident Summary							
A VA employee took home a list with Veterans' information, including the full SSN, to have his spouse help him develop a Word document from the list. The employee tried to email the completed Word document to his VA email account but the VA server rejected it.							
Incident Update							
10/26/10: The PO checked with the HIMS Chief who said the list included 180 Veterans' information. All the documents are back in the hands of the HIMS Chief. She has consulted with HR on the matter and will counsel the employee. One hundred and eighty (180) Veterans will receive a letter offering credit protection services.							
Resolution							
The letter was sent to the affected Veterans.							

Total number of lost Blackberry incidents	22
Total number of internal un-encrypted e-mail incidents	79
Total number of Mis-Handling Incidents	79
Total number of Mis-Mailed Incidents	115
Total number of Mis-Mailed CMOP Incidents	10
Total number of IT Equipment Inventory Incidents	2
Total number of Missing/Stolen PC Incidents	4
Total number of Missing/Stolen Laptop Incidents	10 (all encrypted)