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

August 6 - September 2, 2012

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000078795	Mishandled/ Misused Physical or Verbal Information	VISN 11 Detroit, MI	8/6/2012	8/8/2012	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
VANSOC0578851	8/6/2012	INC000000229112	N/A	N/A	N/A		1

Incident Summary

Veteran A received a letter with the name and medical diagnosis information that belonged to Veteran B.

Incident Update

08/06/12:
Veteran B will be sent a HIPAA notification letter since his medical information was disclosed to Veteran A.

NOTE: There were a total of 110 Mis-Mailed incidents this reporting period. Because of repetition, the other 109 are not included in this report, but are included in the "Mis-Mailed Incidents" count at the end of this report. In all incidents, the Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

The supervisor has conducted training with all staff on the need to review all documents before mailing to insure mis-mailings do not occur. Veteran B was sent a notification letter.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000078831	Mishandled/ Misused Physical or Verbal Information	VISN 19 Sheridan, WY	8/6/2012		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
VANSOC0578956	8/6/2012	INC000000229276	N/A	N/A	N/A	8	154

Incident Summary

An employee while in the restroom saw papers under a stack of paper towels. Upon review it was discovered there were two documents; both printed 07/18/12 at 6:37 a.m..

The first document was a Veteran Patient Roster containing the full name and last four numbers of the Patients' Social Security Number (SSN), admit and transfer dates, ward where patient was located, length of stay, what specialty the patient was in, count of authorized absences, count of passes taken, unauthorized absences, and absent sick in hospital count. This list included 162 Veteran's that were in the hospital on 07/18/12

The second document that was found was the Opt-Out Listing; this document has a total of 8 Patients and is a subset of the first document. This document included full name, full SSN and the ward where the patient was.

This matter is still being investigated to determine who it might have been printed for and why.

Incident Update

08/07/12:
It is unknown how long the documents were in the restroom. They were found on a stack of paper towels with a bundle of paper towels on top of them, on a supply shelf. The restroom is open to both staff and visitors/patients. It is a low traffic area. The documents were found at 2:30 pm on 8/6/12.

08/14/12:
Since there is no way to tell how long the documents were in the public accessible restroom, 8 letters of credit monitoring will be sent, and 154 HIPAA notifications will be sent to the Veterans/Paitents.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000078851	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Hines, IL	8/7/2012		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
VANSOC0579008	8/7/2012	INC000000229378	N/A	N/A	N/A		1

Incident Summary

Patient A received a Medline Industries medical supply intended for Patient B. Patient B's name, address, and type of medical supply were compromised. Patient A reported the incident to the medical center and a replacement has been requested for Patient B. Great Lakes Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a Medline packing error. The packing error has been reported to Medline for investigation and corrective action.

Incident Update

08/07/12:
Patient B will be sent a notification letter due to Protected Health Information (PHI) being exposed.

NOTE: There were a total of 4 Mis-Mailed CMOP incidents out of 6,136,074 total packages (9,214,012 total prescriptions) mailed out for this reporting period. Because of repetition, the other 3 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
SPE000000079098	Mishandled/ Misused Physical or Verbal Information	VISN 20 Seattle, WA	8/13/2012	8/17/2012	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
VANSOC0579617	8/13/2012	INC000000230481	N/A	N/A	N/A	1	

Incident Summary

Patient A was recently discharged from the domiciliary. Upon discharged, he was mistakenly given a bag of medications that belonged to Patient B. Both patients have the same last name. The bag of medications was brought in by Patient B at the time of his admission to the domiciliary. The pharmacist contacted Patient A and he replied he would come into the pharmacy to return the bag. At the present time, he has not returned the medications. The information in the bag included Patient B's full SSN.

Incident Update

08/13/12:
Patient B will be sent a letter offering credit protection services.

NOTE: There were a total of 114 Mis-Handling incidents this reporting period. Because of repetition, the other 113 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

Pharmacy has retrained all staff to double-check SSN and names prior to releasing any items upon discharge, as there are instances when you may have more than one individual with the same name admitted to the same ward.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000079133	Missing/Stolen Equipment	VISN 10 Chillicothe, OH	8/14/2012	8/27/2012	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
VANSOC0579688	8/14/2012	INC000000230652	N/A	N/A	N/A		

Incident Summary

A greenhouse was broken into and a desktop computer, printer and telephone were stolen. The VA Police are currently investigating. The Medical Center Director has been informed. The Facility Chief Information Officer (CIO), Information Security Officer (ISO), and Privacy Officer (PO) have also been informed. The VA employee uses the computer to enter certain patient data but no personally identifiable information (PII) or protected health information (PHI) was stored on the computer.

Incident Update

08/14/12:
No data breach is believed to have occurred. The desktop computer was used to enter in Compensated Work Therapy (CWT) information into a spreadsheet stored on a network drive, and is not believed to have stored any PII or PHI.

08/24/12:
A Report of Survey (RoS) was initiated.

Resolution

No data breach occurred.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000079145	Missing/Stolen Equipment	VISN 16 Jackson, MS	8/14/2012	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
VANSOC0579709	8/14/2012	INC000000230752	N/A	N/A	N/A		

Incident Summary

A VA workstation that resides on the VA network extension at University Medical Center (UMC) was discovered missing by the UMC techs in their lab area. It is unclear if it was actually stolen, removed by UMC IT by mistake or for any other reason. The UMC Police have been contacted.

Incident Update

08/16/12:
No data breach is believed to have occurred. The equipment was used for CPRS access to load results. No personally identifiable information (PII) or protected health information (PHI) was stored locally. All individuals who accessed the PC had VA access credentials and training. The facility Information Security Officer (ISO) is recommending implementing Citrix Access Gateway (CAG) access for future needs.

Resolution

It has been decided to remove VA equipment from the UMC Medical Center and switch the staff that supports the VA there to remote access on the CAG. The last remaining VA equipment is being removed this week. The disposition of the missing PC has not been determined. The disposition of the missing PC has not be determined.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000079146	Missing/Stolen Equipment	VBA Washington, DC	8/14/2012	9/4/2012	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
VANSOC0579710	8/14/2012	INC000000230732	N/A	N/A	N/A		

Incident Summary

The facility reported that their remote office in Indianapolis, called the Portfolio Loan Oversight Unit (PLOU), shipped three boxes containing two PC's and four monitors to the main facility location. The facility received two boxes containing one PC and two monitors, The site is missing 1 PC and two monitors.

UPS was called yesterday and they have issued a trace on the items. According to UPS tracking, it shows that it was picked up from the PLOU and it was scanned in to the UPS facility in Indianapolis, it appears the equipment never left Indianapolis. UPS is tracking the items and will provide an update within 8 -10 business days. Management states that the PC may have been reimaged in 2010 and no one has used the PC since the owner of the device retired in 2010. They also state that there should not be any personally identifiable information (PII) on the PC because of the reimage and non-use of the device. The Facility Chief Information Officer (FCIO), Information Security Officer (ISO) and Privacy Officer (PO) are coordinating efforts with facility and UPS and are continuously fact finding.

Incident Update

08/14/12:
The missing PC was reimaged in 2010 when the prior user retired, and has not been used on the VA network since then. Therefore it is safe to say that the PC does not contain any PII.

Resolution

A claim has been issued. No breach occurred.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000079412	Missing/Stolen Material (Non-Equipment)	VISN 20 Seattle, WA	8/21/2012		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
VANSOC0580014	8/21/2012	INC000000232130	N/A	N/A	N/A		

Incident Summary

Following an IT Equipment Inventory audit, a Report of Survey (RoS) for Puget Sound listed four items that were capable of storing data. Two are cameras used for unknown purposes and two are listed as "training aids" with no other information. The Information Security Officer (ISO) was not able to rule out the "training aids". Request for fact-finding and investigation as to the purpose of the cameras was sent to the Service (Nursing). Per the RoS, a wall-to-wall inventory was done and none of these items were found with the mitigating statement that "Several (four) recent ward relocations, remodeling projects, and construction has adversely affected the staff ability to locate items". At this point, the ISO is trying to find out what the cameras were used for and did they involve protected health information (PHI) and what were the "training aids" and were they data capable at all. The individual identified as using the training aids retired over a year ago and no one seems know to what these items were. The ISO is hoping it turns out to be a CPR doll as the individual identified was the CPR trainer.

Incident Update

08/24/12:
The training aid items appear to be part of the diagnostic cardiology system that may have been loaned to the VA as part of the training in the new equipment. As this is not certain, the staff is continuing to work with the purchasing agent and the vendor to identify the equipment. The two cameras have been found on a sign out log and the two staff who signed out the cameras are being contacted. The employee who signed out one camera is currently on vacation. The employee who signed out the second camera has retired but a new employee was hired to fill that position. That employee has been contacted to discover if she has "inherited" the camera.

08/31/12:
One camera has been found. The employee who signed it out has it in his possession and is using it for his job duties. The equipment inventory will be updated to reflect the correct location. The Service Line is still trying to reach the other employee who may have the other camera.

09/07/12:
UPDATE: No new information. Still waiting for other possible camera owner to return from vacation and still waiting on the Vendor to provide information on the missing device.

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 Category
SPE000000079498	Missing/Stolen Equipment	RCS Lakewood Lakewood, CO	8/23/2012		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
VANSOC0580104	8/23/2012	INC000000232516	N/A	N/A	N/A		

Incident Summary

On 8-23-12 it was reported that a computer was found alongside a road and was turned into The Washington State Department of Veterans Affairs (WDVA). The State agency called the VA. The Information Security Officer spoke with the Tacoma Vet Center Team Leader, who stated that this equipment was not on the Equipment Inventory Listing (EIL) and not on the EIL from the facility. The PC workstation was identified as:

MPC
Model: d865glc-0dyd
Serial:3493796-0001
No other information is known at this time.

EMAIL FROM
Chief Information Officer
WDVA - Information Services
(360) 790-3895

We received a phone call last week from a gentleman from Silverdale, who said that he had found a computer by the side of the road in Port Orchard that he believed belonged to my department. I have that computer in my possession now, and it appears that it belongs to the Federal VA.

Upon starting up this computer, the banner in the attached photo comes up, which is entitled "Dept. of Veterans Affairs Readjustment Counseling Service."

Incident Update

08/28/12:
A citizen returned a computer workstation to The Washington State Department of Veterans Affairs (WDVA). The citizen stated that he found it along the side of a road. The Chief Information Officer for WDVA examined the workstation and determined that it appears to be property of the U.S. Department of Veterans Affairs. The CIO contacted the Tacoma Vet Center who contacted the Information Security Officer form Lakewood, CO. The workstation is not on the Equipment Inventory Listing for either The Vet Center or the Lakewood Community Based Outpatient Clinic (CBOC). At this time it is not known what facility the workstation came from or what data it might contain. A Vet Center employee will be retrieving the workstation and sending it to the Lakewood CBOC for examination by the Information Security Officer (ISO).

Total number of Internal Un-encrypted E-mail Incidents	94
Total number of Mis-Handling Incidents	114
Total number of Mis-Mailed Incidents	110
Total number of Mis-Mailed CMOP Incidents	4
Total number of IT Equipment Inventory Incidents	2
Total number of Missing/Stolen PC Incidents	3
Total number of Missing/Stolen Laptop Incidents	9 (9 encrypted)
Total number of Lost BlackBerry Incidents	24
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	0