

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE00000072441	Mishandled/ Misused Physical or Verbal Information	VBA Buffalo, NY	3/5/2012	3/12/2012	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
VANSOC0552833	3/5/2012	INC000000201117	N/A	N/A	N/A	1	

Incident Summary

On 03/01/12, an email was received from a VA employee at Ft. Drum indicating Veteran A received Veteran B's letter enclosed with her letter from the Buffalo VA Regional Office (RO). On 03/05/12, the Privacy Officer (PO) for the Buffalo RO spoke to Veteran A regarding this incident. Veteran A confirmed that the two letters were not stapled together but were separately enclosed in the envelope. Veteran A returned Veteran B's letter to the VA employee at Ft. Drum, who indicated he would mail the returned letter to Veteran B.

Incident Update

03/05/12:

Veteran B will be sent a letter offering credit protection services. Veteran B's name and full SSN were disclosed in the letter.

NOTE: There were a total of 117 Mis-Mailed incidents this reporting period. Because of repetition, the other 116 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

Based on the information received from Veteran A, it was determined that this incident was the result of an error made by a mailroom employee or other employees assisting with the mail due to the high volume of outgoing mail; however, the PO is unable to identify the specific individual responsible for this error. As a result, all mailroom employees have been reminded of the importance of ensuring that personally identifiable information (PII) is protected and not sent to the wrong Veteran and to take extra care in the processing of outgoing mail. In addition, the PO will continue to review both hand and machine-folded mail each week to further ensure that mis-mailings do not occur.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000072456	Mishandled/ Misused Electronic Information	VISN 20 Portland, OR	3/5/2012		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
VANSOC0552955	3/5/2012	INC000000201236	N/A	N/A	N/A		59

Incident Summary

A Radiology Resident reported that he is unable to locate a personally owned USB storage drive on which he has maintained a spreadsheet of the procedures he has participated in. He reports it has not been seen since late December 2011 or early January 2012. An electronic backup copy of the spreadsheet has been sent to our facility Privacy Officer (PO). The spreadsheet shows the type of procedure, the date, and an identifier for 199 Veterans.

On the copy of the spreadsheet, 138 individuals are identified using the Veteran's last initial and the last 4 digits of their Social Security Number and 59 are identified using their full last name and the last 4 digits of their Social Security Number. The Information is included for procedures dated from 01/05/10 to 10/05/11.

A separate tab on the spreadsheet contained VA and University networks, patient record systems, and radiology package passwords. The facility PO has communicated this information to the University Information Security Officer (ISO) so they are aware of the account vulnerability. The local VA Information Security Officers (ISO) have already requested the passwords be reset.

A review of the VA network access log for the Resident's account shows limited activity since December.

Incident Update

03/09/12:
The 59 Veterans with last names disclosed will be sent HIPAA notification letters.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000072461	Missing/Stolen Equipment	VISN 05 Baltimore, MD	3/5/2012	3/13/2012	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
VANSOC0552975	3/5/2012	INC000000201253	N/A	N/A	N/A		
<p>Incident Summary</p> <p>During the FY12 Information Resource Management (IRM) wall to wall inventory, 4 computers came up missing. The IRM Inventory Specialist believes they are still in VA possession and are just misplaced due to undocumented movement. A Report of Survey (RoS) has been submitted. Staff will continue to search for the computers throughout the facility.</p>							
<p>Incident Update</p> <p>03/09/12: One PC has been found. The three devices still missing include one encrypted laptop and two unencrypted desktop PCs. One was used solely to monitor camera feeds. IRM staff is attempting to determine where the other two items were used. The Information Security Officer (ISO) has been informed that none of the devices were used in patient areas. The facility has written policies and provides training to employees that all data, regardless of sensitivity level is to be stored on the network and not on the local device.</p> <p>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.</p>							
<p>Resolution</p> <p>The Report of Survey was completed and submitted by the service. Staff will continue to look for the computers throughout the facility.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000072546	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Hines, IL	3/6/2012		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
VANSOC0553410	3/6/2012	INC000000201585	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 was 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

03/07/12:

Patient B will be sent a notification letter due to his protected health information (PHI) being disclosed.

NOTE: There were a total of 4 Mis-Mailed CMOP incidents out of 6,299,509 total packages (9,248,025 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		
SPE000000072587	Missing/Stolen Equipment	VISN 01 White River Junction, VT	3/7/2012	3/19/2012	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
VANSOC0553641	3/7/2012	INC000000201790	N/A	N/A	N/A		
Incident Summary							
<p>On 03/07/12, it was brought to the attention of the Information Security Officer (ISO) that an unencrypted Mac book laptop computer purchased in 2005 was unaccounted for. The Mac book was loaned to a VA employee working at a remote location on a Consolidated Memorandum of Receipt (CMR) Equipment Inventory Listing (EIL) for the facility. According to the employee, the computer stopped functioning abruptly in June, 2007. It wouldn't power on at all. This was not related to any damage as it wasn't dropped or mishandled. The employee relates that when she called in 2007 she was told that she was due for another computer anyway, so to discard the nonfunctioning laptop. The employee believes her spouse may have disposed of it at the local landfill. The employee states there was no VA sensitive information on the laptop. She did not have a VA Network account or access to CPRS or VISTA.</p>							
Incident Update							
<p>03/08/12: According to the ISO, the user is remote via telework in Oregon. He is awaiting her signed Report of Contact (ROC) and attempting to validate further.</p>							
Resolution							
<p>The ISO received the ROC. The employee states that she took the laptop to the MAC store and they advised that the motherboard had fried and it was cost prohibitive to fix the device. When the employee advised the VA (does not remember who) she was told to discard the laptop as she was due a new one. The employee again stated there was no personally identifiable information (PII) or protected health information (PHI) on the laptop. She only had articles and educational documents that she was working on stored on the laptop. She was not involved in any direct patient care.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000072681	Missing/Stolen Equipment	VISN 23 Omaha, NE	3/9/2012		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
VANSOC0554089	3/9/2012	INC000000202204	N/A	N/A	N/A		

Incident Summary

On 03/09/12, a nurse at the Lincoln facility reported to the VA Police that a desktop CPU tower was missing. Local PC technicians are in the process of determining if that PC is connected to the VA network from another location.

Incident Update

03/13/12:

An anonymous tip was received by VA Police that someone had bragged about stealing a computer from the VA after an appointment. The VA and local city Police investigated. It was located on Craig's List and Lincoln Police recovered it. The VA Police will retrieve it tomorrow and deliver it to the Information Security Officer (ISO). The computer was not encrypted. VA has not chosen to encrypt desktop computers. Patient records are stored in CPRS on secured servers. Laptops owned by the VA are always encrypted.

03/19/12;

The computer was taken from a room in the clinic which was not used very often. The theft was caught on camera and the local police located the computer on Craig's list and recovered it. There are group policies in place that prevented employees from storing data to the hard drive. The stolen computer has been recovered by Police and is now secured in the Omaha Police Department's evidence room in Omaha. Police have stated that the device will have to remain "out of service" until it is released by the court system.

04/02/12:

A VA local PC technician accessed the PC and examined what files are present. He could only find one file that, based on file name, may have personally identifiable information (PII) or protected health information (PHI). He does not believe that he can examine the contents of the file without altering the metadata of the file. Based on the size of the file (an Excel spreadsheet), it does not appear that a large number of patients' PII or PHI would be in the file.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000072818	Mishandled/ Misused Physical or Verbal Information	VISN 01 White River Junction, VT	3/14/2012	4/5/2012	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
VANSOC0554985	3/14/2012	INC000000202923	N/A	N/A	N/A	118	
Incident Summary							
Several DD214s (Certificate of Release or Discharge from Active Duty) and fee dental approval letters were found in a file cabinet at a Recycling Center and reported to the VA Police. The files were transported by the employees of the Recycling Center to the VA within 30 minutes of discovery.							
Incident Update							
03/15/12: According to the Privacy Officer a total of 118 files were in the cabinet. Each file had a DD214 and the dental approval letters. The letter had full name and full SSN as well as the Veterans' address and year of birth and a descriptive line stated "conditions for which services are requested (description of disability) Dental." Therefore 118 Veterans will receive a letter offering credit protection services.							
Resolution							
Staff conducted a review to verify that all stored furniture does not contain documentation of any kind. The review is complete and no other cases were located in the stored furniture areas. An SOP is being developed to create a system of monitoring to ensure that all unused furniture is empty of all items prior to removal from use.							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000073072	Mishandled/ Misused Physical or Verbal Information	VISN 06 Durham, NC	3/19/2012	3/22/2012	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
VANSOC0556258	3/19/2012	INC000000203687	N/A	N/A	N/A	21	
Incident Summary							
An inpatient ward roster containing information of 21 Veterans was found by a VA employee outside the grounds of a local restaurant within walking distance of the VA Medical Center.							
Incident Update							
03/19/12: All 21 Veterans will be sent letters offering credit protection services. The Veterans' full SSNs and medical information were on the roster.							
NOTE: There were a total of 129 Mis-Handling incidents this reporting period. Because of repetition, the other 128 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 re-took the privacy training, received a verbal warning and his supervisor is taking the time to alert the entire staff of the importance of not leaving the facility with inpatient ward rosters.							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE00000073076	Mishandled/ Misused Physical or Verbal Information	VISN 23 Omaha, NE	3/19/2012		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
VANSOC0556300	3/19/2012	INC000000203677	N/A	N/A	N/A	130	13

Incident Summary

While VA Police were conducting security checks of the exterior buildings, they encountered a man going through a shredding container behind an out building. The man fled off campus when he saw the Police. It is unknown if the suspect fled with any items from the containers. The Police stated that the bin contained contracts, emails and patient information.

Incident Update

03/20/12:

The VA Police originally reported that less than 50 documents were in the shred bin, but after the Privacy Officer reviewed them, she found individually identifiable information for 126 Veterans. Some of these documents have names, full SSNs and dates of birth. Others have names and last four of SSN or names and address. The VA Police notified OIG who declined the case. There are no cameras that view the area where the shred bin was. The shred bin was not locked and was not supposed to be located outside.

03/30/12:

The final counts are 130 Veterans with full SSN disclosed and 13 Veterans with only name and address on the documents. The 130 will be offered credit protection services and the 13 will be sent letters of notification.

Resolution

The Privacy Officer educated the staff in the department. With the support of the Director's office, the facility also immediately implemented 100% shredding of paper in the facility. An email was sent out to all staff. The facility changed the shred contract to allow for more volume and is ordering more shred bins from the contractor.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000073343	Mishandled/ Misused Physical or Verbal Information	VISN 09 Memphis, TN	3/26/2012		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
VANSOC0558093	3/26/2012	INC000000205118	N/A	N/A	N/A		80

Incident Summary

Over the weekend Contractors came in to the Spinal Cord Injury Clinic and waxed the floors. When the Social Worker arrived this morning her office door was open and items were moved around in the office and were not in the correct place. Her computer was disconnected and off line. As she started to put things at their right place, she realized the Fee Basis Home Health and Caregiver's list she had flipped over on the tack board was missing. The list had patients' full names and last four of their SSN, along with the caregiver's name and the name of the agency they work for. The list had about 80 patients names on it. Meanwhile, the facility Environmental Management Service Acting Chief is contacting the Contractor to follow up on this incident.

Incident Update

03/27/12:

All 80 Veterans will be sent a notification letter. There was a follow up on this incident by Acting Chief of Facility Environmental Management Service with the Contractor. The Contractor acknowledged that his staff came to the Memphis VAMC over the weekend to perform their assigned duties. The Contractor stated, he believes if a page (list of patient names) is missing from a bulletin board it was most probably an accident. He stated his staff always strip and wax floors. They bring in large fans that blow with a great deal of force to dry after they have stripped the floor. He is guessing, but he stated it may have been when they turned on one of the fans to start drying the floor that the incident happened. He believes there may have been such a force as to have blown some papers off the bulletin board. If this happened and the paper hit the wet floor which had stripper on it, the paper would have gotten into the stripper and the ink would have run all over the paper, as stripper destroys everything in its path. If that happened the only option would have been to throw the paper(s) away, as they would have been illegible after that. There wouldn't have even been a reason to dry them out and shred them as there just wouldn't be anything on the page but runny ink. The Contractor will check with his employees this morning to ascertain the facts and circumstances that may have led to this incident. Memphis VAMC Facility Management Service will follow up with the Contractor to see if there is any further information that can be used to update this case.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000073348	Missing/Stolen Equipment	VISN 22 Los Angeles, CA	3/26/2012		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
VANSOC0558117	3/26/2012	INC000000205131	N/A	N/A	N/A		
<p>Incident Summary</p> <p>A Pharmacy Technician reported that when she arrived to work at 8:00 AM, she noticed that the computer was missing and reported the missing computer to her Supervisor. The Supervisor then notified an IT Specialist. The computer was last seen by network scanning on 03/25/12 at 3:18 PM. The IT Specialist stated that the computer could have been taken anytime between 3:18 PM and 8:00 AM.</p>							
<p>Incident Update</p> <p>03/28/12: The machine is still missing and the investigation continues. It has not been determined if the computer was stolen at this point. VA Police have been notified and are conducting the investigation. There is policy in place to require users to save to a network location, not locally. Employees can circumvent the policy and settings, but the risk of this is low. A Report of Survey will be completed when the loss is confirmed.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000073533	Mishandled/ Misused Physical or Verbal Information	VBA Seattle, WA	3/30/2012		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
VANSOC0559239	3/30/2012	INC000000206072	3/30/2012	Yes	Pending	55	
<p>Incident Summary A Seattle VARO's Assistant Vocational Rehabilitation and Employment Officer's (AVREO) vehicle was broken into and Veterans' personally identifiable information (PII) was stolen on 03/29/12.</p> <p>On the way home from work on 03/29/12, the AVREO stopped to eat dinner. Her vehicle was parked in the shopping center parking lot from 6:20 PM to 9:30 PM. Upon returning to the vehicle, she found the driver's side window of the vehicle had been shattered and her tote bag and lunch sack were missing. The contents of the bag included a personal planner containing a government travel card, passport, and personal information. She was scheduled to work at home on 3/30/12 so she also had documents and data to complete a Division Systematic Analysis of Operations (SAO). This included the full name, full SSN and file number for 55 identified Veterans. The material had not been placed into a locking red bag as required.</p> <p>The AVREO immediately contacted the police and filed a Police Report of the break-in and theft. She also contacted her immediate supervisor, the Seattle Vocational Rehabilitation and Employment Officer. She contacted the credit card company to report the theft and cancel the government credit card. They provided information that there had been two attempts to use the card at two different gas stations. The AVREO contacted the gas stations to inquire about possible surveillance footage. One indicated they do have cameras; this information was provided to the police and added to the report.</p> <p>On 03/30/12, at 11:50 AM, the AVREO received a phone call from an individual stating he had found her planner. As a result of this event, the Seattle VR&E Officer reminded all VR&E staff members of the importance of properly securing Veterans' PII.</p>							
<p>Incident Update 04/02/12: Fifty-five Veterans will be sent letters offering credit protection services.</p>							

Total number of Internal Un-encrypted E-mail Incidents	84
Total number of Mis-Handling Incidents	129
Total number of Mis-Mailed Incidents	117
Total number of Mis-Mailed CMOP Incidents	4
Total number of IT Equipment Inventory Incidents	4
Total number of Missing/Stolen PC Incidents	3
Total number of Missing/Stolen Laptop Incidents	7 (6 encrypted)
Total number of Lost BlackBerry Incidents	22
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	2