

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000073569	Mishandled/ Misused Physical or Verbal Information	VISN 09 Huntington, WV	4/2/2012	4/12/2012	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
VANSOC0559600	4/2/2012	INC000000206255	N/A	N/A	N/A	10	

Incident Summary

Twenty lab specimens for eight patients at a Community Based Outpatient Clinic (CBOC) that were to be transported to the VA Medical Center cannot be located. A copy of the manifest would contain the patients' names and labs ordered, and the specimen tubes would have the full SSNs on them. This was discovered 03/29/12 but not reported to the Privacy Officer (PO) or Information Security Officer (ISO) until today. Employees conducted a thorough search of the CBOC lab and the transport vehicles involved but have been unable to find the missing specimens.

Incident Update

04/02/12:

Eight Veterans will be sent a letter offering credit protection services due to full name and full SSN being disclosed.

04/09/12:

After a final count, the total number of Veterans affected is 10. Those ten Veterans will receive a letter offering credit protection services.

NOTE: There were a total of 95 Mis-Handling incidents this reporting period. Because of repetition, the other 94 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 acceptance of specimens will be documented so the transport can be tracked in the future.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE00000073579	Mishandled/ Misused Electronic Information	VISN 23 Iowa City, IA	4/2/2012	4/26/2012	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
VANSOC0559646	4/2/2012	INC000000206289	N/A	N/A	N/A	76	

Incident Summary

A VA Clinic medical laptop was left unsecured in a room with public access. The laptop had no VA image, no VA security, and no VA account authentication. The laptop used a generic non-password protected account. The hard drive was unencrypted. The laptop contained 86 patients' records including their first and last name, date of birth, admission date, and last four digits of the social security number. This was reported by VA staff.

Incident Update

04/03/12:

The laptop was in a common room for several months. When the laptop was turned on, the clinical application which held the data opened automatically. All 86 patients will be sent letters offering credit protection services.

04/17/12:

The final count of patients' information stored on the laptop after removing duplicates is 76. Therefore the 76 patients will receive a letter offering credit protection services.

Resolution

An IT Help Desk Ticket has been entered to have the laptop encrypted, pending installation of the encryption by IT Service Delivery and Engineering (SD&E).

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000073618	Mishandled/ Misused Physical or Verbal Information	VISN 19 Fort Harrison, MT	4/3/2012	4/25/2012	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
VANSOC0559967	4/3/2012	INC000000206492	N/A	N/A	N/A	211	168
Incident Summary							
A box of patient records was found unsecured in an unused outbuilding on the medical center campus.							
Incident Update							
04/03/12: The Privacy Officer (PO) is determining the exact number of records, and where they might have come from.							
04/11/12: The Data Breach Core Team determined that the 392 individuals whose records were out of VA control in the out building will be sent letters offering credit protection services due to full name and full SSN being exposed.							
04/12/12: All address information was reviewed and updated to reflect the most current address in VISTA. The number of Veterans went down from 392 to 385 as more duplicate records were identified. Additionally, 8 Veterans are no longer in VISTA. The PO spoke with the Enrollment Coordinator and was told in the 1990s that if Veterans were not being seen, they were deleted from the system, necessitating re-enrollment. The number of affected Veterans who can be located is 379.							
04/13/12: The spreadsheet has been completed. There are 211 Veterans who are living who will receive letters offering credit protection services and 168 who are deceased whose next of kin (NOK) will receive NOK notification letters. The PO is unable to determine how the documents came to be in the outbuilding.							
Resolution							
The Information Security Officer (ISO) interviewed the Veteran who found these records and his provider. The Veteran first discovered them on 04/02/12 after hours, but waited until lunch time the next day to report them to his provider. He went through some of the records and stated that they looked weather-beaten. He does not believe anyone went there between the time he found them and when he and his provider saw them. Upon the provider's return to the office, she immediately contacted the ISO. The ISO discovered that the structure has been there at least 14 years. There is no evidence of people going in and out recently.							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000073687	Missing/Stolen Equipment	VISN 04 Coatesville, PA	4/4/2012	4/24/2012	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
VANSOC0560263	4/4/2012	INC000000206798	N/A	No	N/A		

Incident Summary

On 04/04/12, Coatesville OIT completed the annual equipment inventory list (EIL) review and discovered that 3 desktop computers and 1 personal data assistant (PDA) couldn't be located. This equipment was last accounted for in November 2011. The PDA is not suspected to contain patient information. The 3 desktops are not thought to have personally identifiable information (PII) however no confirmation can be made either way at this time. Coatesville VAMC Police, OIT, Information Security Officer (ISO) and Acquisitions are investigating and in the process of recovering the serial numbers and other identifying information for these missing computers. Coatesville staff members from several departments are currently looking for the missing equipment.

Incident Update

04/09/12:
The missing PDA and 1 PC were found on 04/05/12. The other two computers are still missing:

Resolution

To attempt to prevent a reoccurrence of this incident, the Chief Information Officer (CIO) will implement better IT inventory control procedures and train OIT staff on the new process.

The 2 remaining desktops are not thought to have personally identifiable information (PII) however no confirmation can be made either way at this time. A thorough search of the facility has been conducted, the paperwork for the loss of PCs has been filed, and a Police Report was filed. Disposition is lost or stolen at this time.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE00000073688	Missing/Stolen Equipment	VISN 01 Bedford, MA	4/4/2012		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
VANSOC0560267	4/4/2012	INC000000206786	N/A	N/A	N/A		

Incident Summary

At approximately 4:30 PM on 04/04/12, IT received a call from the Administrator of the Day (AOD) that a workstation computer was missing from the Medical Officer of the Day (MOD) call room in building 78, Room 1170. The VA Police and Network and Security Operations Center (NSOC) have been notified with the preliminary information. It is unknown if this device is stolen or missing. IT was notified by the AOD that Facility Management Service was working in the area last evening which could indicate that the device may have been moved, but IT cannot rule out that the device was stolen.

Incident Update

04/05/12:

Information obtained from the Medical Administrative Assistant indicates that the device was last seen on 04/04/12 at approximately 8:00 AM by the overnight MOD. It appears that the MOD call room was unlocked during the day on 04/04/12 which would have allowed anyone from 8:00 AM to 4:30 PM to enter the call room and take the device in question. IT is currently pinging the device in an attempted to determine whether the device was moved from its location to another on the facility grounds. VA Police have begun their investigation.

04/09/12:

There is no further information related to this ticket at this time. The VA Police are still investigating this incident.

04/10/12:

On 04/09/12, IT Operations advised that they have not been able to locate this device on the network. This case is still being investigated by VA Police.

05/01/12:

There is no further information to report on this ticket. VA Police have no leads and IT Operations is not able to ping the device on the network.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000073844	Mishandled/ Misused Physical or Verbal Information	VBA Lincoln, NE	4/9/2012	4/10/2012	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
VANSOC0561030	4/9/2012	INC000000207392	N/A	N/A	N/A	1	
<p>Incident Summary A letter sent to Veteran A also included a letter intended for Veteran B. Veteran A returned the letter intended for Veteran B. The letter sent to Veteran A included Veteran B's name, address and SSN.</p>							
<p>Incident Update 04/09/12: Veteran B will be sent a letter offering credit protection services.</p> <p>NOTE: There were a total of 122 Mis-Mailed incidents this reporting period. Because of repetition, the other 121 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.</p>							
<p>Resolution The Privacy Officer (PO) notified the VBA coach and employees of the importance of checking correspondence and ensuring that the correct letters are going to the correct Veterans.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE00000073880	Missing/Stolen Equipment	VISN 07 Augusta, GA	4/10/2012		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
VANSOC0561248	4/10/2012	INC000000207609	N/A	N/A	N/A		

Incident Summary

On Tuesday, 04/10/12 the Privacy Officer (PO) was contacted by the PO at an affiliate medical center regarding a stolen personal laptop. A former Chief Resident, who is now an Attending, reported that on 03/30/12, his personal laptop was stolen from his office at the affiliate hospital while he was next door in an exam room. The Police were contacted and a report was filed. According to the physician, the laptop contained both the affiliate's and VA's data in the form of Word documents and Excel spreadsheets from 2008-2009 during his stint as Chief Resident. The VA files have not been reviewed, but are reported to pertain mainly to undictated discharge summaries with the following data elements: name, date of discharge, last 4 digits of the SSN, length of stay, location at the VA, and Resident's name. No other VA medical information is reportedly involved. The laptop has not been recovered. The exact number of VA patients impacted is unknown. Copies of the Police Report and further details will be provided to the PO.

Incident Update

04/16/12:

The PO has received the copies of the files that were on the laptop, and a review is in process. The PO will update the IRT as soon as a final count is determined.

04/26/12:

The PO's review of the 39 files is complete. The files contain protected health information on 824 Veteran patients in the form of undictated hospital summaries from June 2008 through October 2009.

04/30/12:

The 824 records are being reviewed to identify the active versus deceased Veterans, in order to determine whether they will receive offers for credit protection services or next of kin notification.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000073929	Mishandled/ Misused Physical or Verbal Information	VISN 19 Denver, CO	4/10/2012		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
VANSOC0563864	4/20/2012	INC000000209677	N/A	N/A	N/A		
<p>Incident Summary</p> <p>The Eastern Colorado Health Care System was notified by the Western Office of Research Oversight (ORO) that a VA Research protocol dating from 2004 to 2007, may have disclosed up to 69 Veteran participants' information without proper notification. It is not known what information was or was not released inappropriately at this time. An internal investigation has been launched.</p>							
<p>Incident Update</p> <p>04/20/12: The Research Department is still pulling the appropriate data together to complete the investigation.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE00000073949	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Dallas, TX	4/11/2012		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
VANSOC0561517	4/11/2012	INC000000207855	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. Dallas 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

04/11/12:
Veteran B will be sent a notification letter.

NOTE: There were a total of 2 Mis-Mailed CMOP incidents out of 6,324,163 total packages (9,371,524 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.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE00000073960	Mishandled/ Misused Electronic Information	VISN 16 Muskogee, OK	4/11/2012		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
VANSOC0561572	4/11/2012	INC000000207880	N/A	N/A	N/A	91	5

Incident Summary

VA shared files were sent to users by accident. The users who opened the files looked at other staff and co-workers' performance evaluations and other personal documents, including the full SSN. It was reported that one employee sent the information to her home computer and shared it with other employees.

Incident Update

04/16/12:

The Privacy Officer (PO) and Information Security Officer (ISO) will attempt to interview the employee who shared other employees' information with co-workers. IT staff have removed the shared folder. The ISO will meet with the service line director to inform her of the accusation against the employee.

04/16/12:

According to the ISO, approximately 178 employees' information was on the share drive. The IT Department is unable to tell how many individuals looked at the records, or what was copied. At this time it is unknown if the information is still on the home computer. The employee has not been interviewed due to the employee working night shift. The ISO and the PO is scheduled to interview the employee this week. The service chief has been notified and will be dealing with any personnel/administrative actions.

04/16/12:

The number of employees affected is over 200 past and present employees.

04/17/12:

The PO and ISO interviewed the employee concerning information sent home to her computer. The employee stated she sent it home so she could call the IT technician later to confirm what information was exposed and where on the portal it was. She also stated she was unable to open the attachment that she sent to her home computer. The IT Department was contacted to remove files or correct permission.

04/30/12:

The revised counts (due to duplicates) are 91 Employees had full SSN exposed, and 5 Employees had name and partial SSN exposed, therefore 91 Employees will receive a letter offering credit protection services and 5 Employees will receive a general notification letter.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000074580	Missing/Stolen Equipment	VISN 18 Albuquerque, NM	4/25/2012		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
VANSOC0564867	4/25/2012	INC000000210363	N/A	N/A	N/A		
<p>Incident Summary</p> <p>Between November and December 2011 the Cardiac Catheterization Lab was relocating from one office space to another. On or about 12/10/11, the Cardiac Catheterization Lab staff noticed that a Phillips Xper Personal Assistant Workstation, which included 2 monitors and a Dell tower, a specialized keyboard and mouse, was unaccounted for. The Cardiac Catheterization lab staff reported this on 04/23/12 to the VA Police Service who are conducting fact finding. The Police Service contacted the Information Security Officer (ISO) and provided this information.</p> <p>One monitor and keyboard was found by the Police Officer in a housekeeping closet that used to belong to the Cardiac Catheterization Lab prior to moving spaces. The Dell tower is still unaccounted for. The Dell tower had test data and did not contain personally identifiable information (PII) or protected health information (PHI). The Police Officer is attempting to contact Phillips to see if they picked up the equipment which may have been on loan.</p>							
<p>Incident Update</p> <p>04/25/12: The delay in reporting the equipment missing was due to the staff searching for the equipment. No data breach occurred. The computer did not contain PII or PHI. It only contained test data.</p>							
<p>Resolution</p> <p>Management is considering a personnel action for failure to report missing equipment timely.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000074585	Missing/Stolen Equipment	VISN 02 Albany, NY	4/25/2012		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
VANSOC0564902	4/25/2012	INC000000210390	N/A	N/A	N/A		

Incident Summary

It was reported that 2 new laptops are missing. The laptops were not configured for VA use and were not encrypted. To the best of our knowledge neither contained personally identifiable information (PII) or protected health information (PHI).

Incident Update

04/25/12:

The laptops were new and not encrypted. Neither laptop contained PII or PHI. The laptops were part of the national IT laptop refresh, (IT Hardware) they were to replace the 2 laptops in the Police Cars. It appears an equipment order was delivered to the Medical Center, but the laptops were not entered into the Albany Laptop Equipment Inventory List (EIL) or delivered to the appropriate location. The same purchase order had computer hardware for Albany and the Field Office. The facility is trying to find out if the laptops were actually received and if so were they delivered to the appropriate location, Contracting is coordinating this process because the laptops were never received in Albany IT or accepted on their Equipment inventory list. VA Police and Contracting are still investigating.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000074617	Unauthorized Electronic Access	VISN 19 Grand Junction, CO	4/25/2012		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
VANSOC0565060	4/25/2012	INC000000210561	N/A	N/A	N/A		

Incident Summary

The local union president brought up an allegation to the Information Security Officer (ISO), Alternate Privacy Officer (PO), and Human Resources (HR) Supervisor today. The allegation is that two VA employees from the lab let a non VA employee come into the lab (a sensitive area) and utilize computer resources for the past two years on nights and weekends. An investigation will need to be conducted. At this point it is an allegation only.

Incident Update

04/27/12:

The Medical Center Director authorized an Administrative Investigation Board (AIB) for this incident.

05/02/12:

The PO spoke to member of AIB team yesterday. The AIB is interviewing employees Monday through Wednesday of this week.

05/04/12:

The AIB team is waiting for transcripts of the interviews to come back, and will re-convene next Tuesday 05/08/12.

Total number of Internal Un-encrypted E-mail Incidents	100
Total number of Mis-Handling Incidents	95
Total number of Mis-Mailed Incidents	122
Total number of Mis-Mailed CMOP Incidents	2
Total number of IT Equipment Inventory Incidents	1
Total number of Missing/Stolen PC Incidents	2
Total number of Missing/Stolen Laptop Incidents	9
Total number of Lost BlackBerry Incidents	20
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	0

