



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
Jan 3 - 30, 2011**

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE000000056610	Mishandled/ Misused Physical or Verbal Information		VBA Atlanta, GA		1/3/2011	1/13/2011	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
	1/3/2011	INC000000129119	N/A	N/A	N/A	1	0
Incident Summary A two-page letter addressed to Veteran A included Veteran B's name and SSN on top of the second page. Veteran A contacted the VA to report the error.							
Incident Update 01/04/11: Veteran B will receive a letter offering credit protection services.							
NOTE: There were a total of 97 Mis-Mailed incidents this reporting period. Because of repetition, the other 96 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 employee was counseled and the corrected letter sent to Veteran A.							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000056693	Mishandled/ Misused Electronic Information	VISN 18 Phoenix, AZ	1/4/2011		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
	1/4/2011	INC000000129380	N/A	N/A	N/A		

Incident Summary

On 01/04/11, at approximately 1:00 PM, a VA employee emailed and phoned the Information Security Officer to ask how she could safely remove VA data from a personally owned computer tower. The VA employee advised she was on contract for the Cleveland VAMC as a remote coder three years ago. Three years ago the Rescue software was not available. She advised that her inquiry was sparked by her interest in giving her tower to a friend. The Cleveland ISOs have been notified. One of the Cleveland ISOs informed the Phoenix ISO that she felt the user can use WIPEDRIVE. She stated she would inquire about additional means of wiping the drive from an IRM representative from Cleveland.

Incident Update

01/07/11:

The user brought her personal computer in to be checked and to have any VA data removed. The local IRM staff reviewed the tower and reported that nothing VA related was found. Therefore IRM is currently running a delete file recovery program, to further ensure no data was on the device.

02/02/11:

The hard drive and associated paperwork was forwarded to VANSOC via Fed Ex to have the drive examined forensically.

02/07/11:

VANSOC received the hard drive and it is currently secured in the evidence locker until VANSOC can examine it.

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE000000056853	Mishandled/ Misused Physical or Verbal Information		VISN 16 Muskogee, OK		1/7/2011	1/18/2011	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
	1/7/2011	INC000000129926	N/A	N/A	N/A	73	6
<p>Incident Summary</p> <p>A canteen employee found a copy of the Inpatient Roster in the canteen cafe and gave it to the Service Chief. The roster includes the patients' full name, SSN, DOB and PHI.</p>							
<p>Incident Update</p> <p>01/11/11: There were seventy nine names on the list. That includes two with the last initial, last four digits of the SSN and the diagnosis and four others with the last name & last four digits of the SSN. The roster was there less than 4 hours. Canteen employees, Veterans, and VA employees may have seen the list. Seventy three patients will receive a letter offering credit protection services and six patients will receive a letter of notification.</p>							
<p>Resolution</p> <p>The Service Chief identified the employee responsible for leaving the list unattended and provided verbal counseling. The credit protection and notification letters were sent.</p>							

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE000000056865	Missing/Stolen Material (Non-Equipment)		VISN 01 Providence, RI		1/7/2011	1/12/2011	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
	1/7/2011	INC000000129963	N/A	N/A	N/A		
<p>Incident Summary</p> <p>On 01/05/11, the VA Police received a call from the Section Chief of Podiatry informing them that one of the two leased laptops was missing. The laptop was part of a medical device and was not encrypted. It was a standalone system that housed a foot pressure analyzer application called ISTEP. This laptop was hooked up to a scanner that the patient could stand on. Only the patient's gender was entered into the application and the computer would display the patient's shoe size and where the pressure points were on their feet. The display was not printed or saved. There was no other patient information stored on the laptop. The Section Chief reported last seeing the laptop on or about 12/20/10 lying on the counter. The laptops were supposed to be locked in an overhead compartment of his desk. A VA Police Report was filed.</p>							
<p>Incident Update</p> <p>01/10/11: No data breach occurred since nothing was stored on the laptop. The application was only used 6 to 8 times.</p>							
<p>Resolution</p> <p>The ISO will speak to the Section Chief on the importance of locking up equipment.</p>							

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE00000057094	Privacy		VISN 16 Houston, TX		1/14/2011	2/2/2011	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
	N/A	N/A	N/A	N/A	N/A	115	
<p>Incident Summary</p> <p>The Pharmacy Administrative Officer reported that her emergency call back "cascade" report has been stored on the Pharmacy's shared drive since 2005 and has been routinely updated as the employees' information changed. The report is used when it is necessary to call back employees in case of an emergency. The report is in an excel format and contained the employees' full name, full social security number, home address, and all contact telephone numbers. The document should have been placed in a secured folder with access restricted to supervisors and leads and not the entire department. The ISO is unable to determine how many of the employees actually accessed the report. The document has been relocated to a secure folder and the SSN has been removed. There were a total of 141 names on the form but 26 only had the employee's name and no other information.</p>							
<p>Incident Update</p> <p>01/20/11: One hundred and fifteen employees will receive a letter offering credit protection services.</p>							
<p>Resolution</p> <p>A broadcast message was sent to all medical center staff asking them to review all shared folders and files to which they currently have access. Staff was asked to ensure that they still need the access as part of their duties and if they do not need the access, to notify their supervisor. The SSN was removed from the cascade listing and the listing was placed in secure folder the can only be accessed by supervisors.</p>							

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE000000057097	Missing/Stolen Material (Non-Equipment)		VISN 06 Durham, NC		1/14/2011	1/24/2011	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
	1/14/2011	INC000000130928	N/A	N/A	N/A		
<p>Incident Summary</p> <p>On 01/03/11, the medical Automated Data Processing Application Coordinator (ADPAC) was notified that two VA desktop workstations and three monitors were missing from a physicians' workroom at the Durham VAMC. The workroom is heavily traveled with a large number of residents who use the various workstations. The ADPAC contacted the Durham OI&T staff to determine if the workstations and monitors had been removed by OI&T. On 01/10/11, the medical ADPAC followed up with the local OI&T again to determine if the equipment had been removed by OI&T staff. On 01/12/11, OI&T determined that no work order had been received in regards to those workstations. The equipment was reported as missing/stolen to VA Police and a Report of Survey was initiated. Due to the holiday schedule, the workstations could have been taken anytime between 12/23/10 and 01/01/11. It is standard guidance that no information should be saved to the hard drive but the ISO is unable to determine if any PII/PHI was stored on the hard drives of the workstations. The Medical Service Chief, Authorizing Official, ISO and Executive Leadership were informed of this incident.</p>							
<p>Incident Update</p> <p>01/18/11: There were no cameras in the area.</p> <p>01/21/11: The ISO was unable to interview the residents who use this room because they rotate at a high rate. The residents who are currently there were not there before the workstations were stolen. The ISO cannot say with any degree of certainty that nothing was stored on these hard drives although the local policy directs staff to store data only to the network drives.</p>							
<p>Resolution</p> <p>The VA Police filed a Police Report.</p>							

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE000000057196	Mishandled/ Misused Physical or Verbal Information		VISN 11 Danville, IL		1/18/2011	1/25/2011	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
	1/18/2011	INC000000131200	N/A	N/A	N/A	1	
<p>Incident Summary</p> <p>An inpatient arm band was discovered attached to a wheel chair in the wheelchair repair clinic at VA Illiana Health Care System. The arm band contained a patient's name, full social security number and date of birth. The wheelchair repair clinic workers are Compensated Work Therapy patients.</p>							
<p>Incident Update</p> <p>01/18/11: The patient will receive a letter offering credit protection services.</p> <p>NOTE: There were a total of 81 Mis-Handling incidents this reporting period. Because of repetition, the other 80 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.</p>							
<p>Resolution</p> <p>The Chief Nurse of the Community Living Center provided education to all staff instructing them not to print out inpatient arm bands for the use of identifying the owner of personal equipment of patients such as wheel chairs, walkers, etc. The credit protection letter was sent to the patient.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000057221	Missing/Stolen Material (Non-Equipment)	VHA CMOP Dallas, TX	1/18/2011	2/2/2011	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
	1/18/2011	INC000000131309	N/A	N/A	N/A		

Incident Summary

Computers and an overhead projector are not accounted for at this time. The number of computers is still being determined. It is believed that the hard drives were removed from the computers and may all be accounted for. It is probable that this equipment was sent as excess to UNICOR, the Federal Prison vendor responsible for excessing IT equipment. IT believes they have the serial numbers and will provide them to Logistics so the EE Numbers can be determined. With the EE numbers, Logistics expects to determine more about the number of computers involved and their possible disposition.

Incident Update

01/21/11:

To date, the following IT equipment is still missing.

30 desktop computers

4 servers

33 printers

50 monitors

2 switches

25 scanners

9 UPS

1 projector

1 television

1 satellite receiver

1 router

2 hubs

A conference call was held. Conferees concluded that records from UNICOR will hopefully account for the equipment and that a National CMOP Asset Management IT Specialist will conduct a wall-to-wall inventory of the Dallas CMOP between 01/25/11 – 01/28/11.

It is believed that no equipment is lost and that this is just a book keeping issue. VA form 2237 (Request, Turn-In and Receipt for Property or Services) will be completed for each item after the fact and UNICOR documentation will be attached to these.

EIL files will be required from now on, as will transfer hand receipts, property loan forms, equipment turn-in sheets, data input into VistA, EE numbers, and barcode labels for inventory. Also, all agreed with a proposal from the National IT CIO CMOP/PBM that all CMOP sites should be inventoried and the chain of control implemented.

01/31/11:

It is believed that the equipment was excessed and shipped to UNICOR. UNICOR has a record of receipt of 25 pallets. Hard drives were removed before shipment and sent out for destruction. CMOP Dallas has the certificates of destruction on file. They did not however annotate the serial number from the PC or server the hard drive was removed from; only the serial number for the hard drive is listed. They have 184 certificates of destruction for hard drives from 9/18/09 to 9/10/2010.

It appears that there was a lack of documentation to clearly annotate the appropriate serial numbers for both the computers and hard drives. The site does have 184 certificates for destruction of hard drives and they do have a history of removing the drives and destroying them properly. The majority of CMOP desktop computers are on our production floor. Data is not saved to the hard drives so no PHI would be present.

CMOP is currently waiting for a list of serial numbers from UNICOR to finalize their investigation. New procedures will be put into place to ensure that the proper documentation is kept for IT inventory. A Report of Survey will be done for any equipment that is deemed missing after the final investigation.

Staff is waiting for the final count and the information from UNICOR. They will not however be able to match hard drives to computer since the matching serial numbers were not documented. As stated above the Facility Chief Information Officer (FCIO) did send out 184 drives to be sanitized and destroyed so by procedure this was done prior to the excess to UNICOR. Also by procedure the computers on the production floor do not allow for data to be saved to the hard drive. They are connected to the production server and are used to verify prescription data against the product being packaged. The FCIO stated that this equipment was removed from the production floor when the new Dell lease came into effect. Once the ISO has a final count, a Report of Survey will be done.

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE000000057235	Missing/Stolen Material (Non-Equipment)		VISN 06 Beckley, WV		1/19/2011		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	Medium No. of Loss Notifications
		N/A	N/A	N/A	N/A		
Incident Summary							
<p>A computer being used in the boiler plant is currently not accounted for. The computer is an older 486x processor that was in use at the boiler plant. The computer was donated to the VA in or about 1996. It is believed that the computer was used to monitor the boiler plant equipment. The computer was last scanned for inventory in April 2010 in the warehouse and documentation is presently reflecting that the computer was turned in for disposal. It is not known at this time if the hard drive was removed, but actions are being taken to verify if the hard drive was or was not removed. There was a meeting with the acting Associate Director, Privacy Officer, CIO and FMSL Chief. Management is aware of this incident and the VA Police are actively looking into this situation.</p>							
Incident Update							
<p>01/21/11: Neither the computer nor the hard drive has been accounted for. The likelihood that there was PII or PHI on device is extremely low since the machine was not connected to the network and was located in the boiler plant which is a non patient care area. It is believed the computer was an interface with a machine in the boiler plant. Since it was last seen in the warehouse for disposal it is believed to have been turned in for disposal but no paper work has been found to confirm it. The investigation continues.</p> <p>01/31/11: The machine was last scanned in the warehouse. The disposition of the machine at this time is unknown. Documentation is being researched to verify if the machine was shipped out and if the hard drive was removed.</p>							

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE00000057306	Mishandled/ Misused Physical or Verbal Information		VHA CMOP Tucson, AZ		1/20/2011	2/4/2011	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
	1/20/2011	INC000000131610	N/A	N/A	N/A		1
<p>Incident Summary</p> <p>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 issued for Patient B. Tucson Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error. The CMOP packer was released from duty by the contracting company due to multiple errors. The process for packing prescriptions at multiple stations is under review and will be revised in an effort to prevent future errors of this nature.</p>							
<p>Incident Update</p> <p>01/04/11: Patient B will receive a notification letter.</p> <p>NOTE: There were a total of 6 Mis-Mailed CMOP incidents out of 5,765,231 total packages (8,521,975 total prescriptions) mailed out for this reporting period. Because of repetition, the other 5 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>							
<p>Resolution</p> <p>The process for packing prescriptions at multiple stations is under review and will be revised in an effort to prevent future errors of this nature.</p>							

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE00000057399	Missing/Stolen Equipment		VISN 22 Long Beach, CA		1/21/2011	1/31/2011	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
	1/21/2011	INC000000131911	N/A	N/A	N/A		
<p>Incident Summary</p> <p>While conducting an inventory, the Manager of Recreation Therapy noticed that a non-GFE, donated laptop was potentially missing on 01/19/11. After discussing the missing laptop with staff and other area employees and patients, the Manager reported the laptop missing on 01/21/11. No one admits to knowledge of the laptop's disappearance. The local Incident Response Team was assembled to discuss and collect details.</p> <p>This laptop was donated for patient bedside usage. Patients used the laptop to access the Internet and for other standalone laptop usage. The laptop was never used to access the VA network. The laptop was normally stored in a secured, locked room in a cabinet that was locked by a combination lock. Only the Manager and two therapists had access to the combination. When the laptop was checked out, it was tracked via a cardex system by the Manager or the two therapists. The VA staff member would then secure the laptop to the patient's bed via a cable lock. The VA Police have been called in to investigate.</p>							
<p>Incident Update</p> <p>01/22/11: The laptop did not store any PII/PHI on it. The laptop was never connected to the VA network. No data breach occurred.</p>							
<p>Resolution</p> <p>The section Chief was instructed by ISO and local Incident Response team to:</p> <ol style="list-style-type: none"> 1) Enhance the current inventory tracking to include: chain of custody type procedures for sign-out, securing of laptop to bedside and sign-in of equipment (i.e., use electronic [online] based tracking document versus current paper method). 2) Conduct more frequent inventory of equipment. 3) Store equipment in single location and more secure location. 							

Security Privacy Ticket Number		Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE000000057451		Missing/Stolen Equipment		VISN 22 Long Beach, CA		1/24/2011	1/26/2011	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	
	1/24/2011	INC000000132059	N/A	N/A	N/A			
Incident Summary								
<p>On 01/23/11 at or about 12:20 PM, 5 computers were delivered to the facility's main IT room located in the basement of Building 126. At 12:30, it was discovered that the hard drive was missing from one computer. Several facility staff members questioned as to whether they had removed the hard drive but all gave negative responses. The incident was reported to VA Police. The missing hard drive contained AGFA proprietary software that makes access to the information more difficult if not impossible.</p>								
Incident Update								
<p>01/24/11: The hard drive was probably in service from 3 to 4 years. It was used to modify Radiology images using the orthopedic medical device PC. The images are only accessible using a USB key, unless the images were saved as JPEG files on the hard drive. Users were not supposed to do this.</p> <p>01/25/11: It is believed that the maximum number of Veterans involved in this is 12. There is an SOP in the Ortho Clinic to remove images from the machine in a timely manner.</p>								
Resolution								
<p>Several exhaustive interviews of all personnel involved in the use of the computer's missing hard drive were conducted by the ISO and the VA Police. Only The Chief, a Physician's Assistant and four Residents had access to the computer and each denied storing any PII or PHI on the hard drive. Additionally, the computer was used to run a program that required the use of a "dongle" which is a hardware device attached to a computer without which a particular software program will not run. The dongle or key was not taken. The ISO and VA Police concluded that no patient information was being stored on this drive at the time of its loss.</p>								

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000057545	Missing/Stolen Equipment	VISN 23 Minneapolis, MN	1/26/2011		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
	1/26/2011	INC000000132420	N/A	N/A	N/A		

Incident Summary

The Minneapolis Information Resource Management (IRM) identified that 5 Bar Code Medication Administration (BCMA) laptops are missing. BCMA laptops are not encrypted since they are used as medical devices. The laptops were identified as missing when all BCMA devices were reconfigured to use a new wireless system installed as part of a national initiative. BCMA laptops are configured to prevent writing to the local drive, which is intended to ensure that no sensitive data is placed on the system.

Incident Update

01/27/11:

The local IRM continues to try to locate these devices. Most, if not all of the BCMA laptop carts were tagged with RFID tags. IRM has reviewed the reports from the RFID system and found that those reports contain 5 more carts than those that have been inventoried manually. They have been able to identify the locations of those 'extra' carts but they are in rooms that IRM has not been able to access because the rooms are in use by patients. IRM intends to go to these locations to identify if these are the missing carts. It is also possible that the laptops were turned in as excess without the proper documentation.

01/28/11:

The RFID reports did not result in finding the laptops. The missing laptops are still under investigation.

02/02/11:

The IRM completed a walk-through inventory and the laptops were not located. The IRM is in the process of doing a warehouse inventory.

Total number of lost Blackberry incidents	24
Total number of internal un-encrypted e-mail incidents	77
Total number of Mis-Handling Incidents	81
Total number of Mis-Mailed Incidents	97
Total number of Mis-Mailed CMOP Incidents	6
Total number of IT Equipment Inventory Incidents	1
Total number of Missing/Stolen PC Incidents	4
Total number of Missing/Stolen Laptop Incidents	9 (6 encrypted)