



---

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**  
**Apr 4 - May 1, 2011**

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE000000060379	Mishandled/ Misused Physical or Verbal Information		VISN 08 Gainesville, FL		4/4/2011	4/18/2011	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
	4/4/2011	INC000000143108	N/A	N/A	N/A		1
<p><b>Incident Summary</b></p> <p>Veteran A received the medication reconciliation summary for Veteran B. Veteran A reported the violation to his Congressman who sent the matter to this facility. Patient Services reported the issue was closed with the Congressional Office. The Privacy Office (PO) will investigate further. The disclosed information included Veteran B's name, address, and medication list.</p>							
<p><b>Incident Update</b></p> <p>04/04/11: Veteran B will be sent a notification letter.</p> <p>05/11/11: To avoid future errors of providing patient medication information to the wrong patients, both the nursing staff and the physicians will check the handouts being given to the patients. During the medication reconciliation process, a patient's medication list is printed and discussed with patient to ensure both the provider and patient are aware of all medication being taken. Either the nurse or physician prints the list and the list is shared with the patient. In this case, the patients had close appointment times and an oversight occurred. In the future, all staff have been directed to review and verify patient demographic information on all documentation prior to discussing and/or giving that information to patients.</p> <p><b>NOTE: There were a total of 118 Mis-Mailed incidents this reporting period. Because of repetition, the other 117 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.</b></p>							
<p><b>Resolution</b></p> <p>It was determined this was unintentional and the result of human error. The responsible physician was counseled and completed refresher VA Privacy and Security training. The Office has taken measures to ensure that this does not happen again.</p>							

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE00000060439	Mishandled/ Misused Physical or Verbal Information		VISN 16 Muskogee, OK		4/5/2011		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
	4/5/2011	INC000000143366	N/A	N/A	N/A	31	
<p><b>Incident Summary</b></p> <p>A copy of a morning report was found by an employee in the Medical Center's Canteen Cafeteria. A nurse left the report in the Canteen. It was there less than 30 minutes. The list contained the full name, SSN, diagnosis, sex, and age of thirty-one (31) inpatient Veterans.</p>							
<p><b>Incident Update</b></p> <p>04/05/11: Thirty-one (31) Veterans will be sent letters offering credit protection services.</p> <p><b>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.</b></p>							
<p><b>Resolution</b></p> <p>The nurse was counseled to be more careful with printed documents. The Privacy Officer (PO) and Information Security Officer (ISO) will remind all staff to print documents only when necessary and to shred documents containing personally identifiable information (PII) or protected health information (PHI).</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000060452	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Charleston, SC	4/5/2011	5/4/2011	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
	4/5/2011	INC000000143418	N/A	N/A	N/A		1

**Incident Summary**

Patient A received two supply items from Medline Industries intended for Patient B. This incident was reported to the Bay Pines VAMC by Patient A and the Bay Pines VAMC reported it to the Consolidated Mail Outpatient Pharmacy (CMOP) on 04/04/11. The item/paperwork contained Patient B's name and supply item name. No SSN data was compromised. The investigation reveals that Patient A and Patient B's orders were processed at Medline.

**Incident Update**

04/05/11:  
Patient B will be sent a notification letter.

**NOTE: There were a total of 7 Mis-Mailed CMOP incidents out of 6,042,763 total packages (8,894,862 total prescriptions) mailed out for this reporting period. Because of repetition, the other 6 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.**

**Resolution**

The packaging error has been reported to Medline for investigation and corrective actions. Medline resent Patient B's supply items.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000060480	Missing/Stolen Equipment	VISN 10 Cleveland, OH	4/5/2011		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
	4/5/2011	INC000000143509	N/A	N/A	N/A		

**Incident Summary**

VA Police reported that a desktop workstation is missing from Building 3 at Brecksville. The employees thought that the workstation might be in Information Resource Management's (IRM) custody since 03/29/11 for repair. The supervisor returned from vacation on 04/05/11 and reported the workstation missing.

**Incident Update**

04/06/11:

According to the Information Security Officer (ISO), interviews with the staff indicate that there was no personally identifiable information (PII) or protected health information (PHI) stored on the computer. The keyboard, mouse, and proprietary central processing unit (CPU) power supply are still in the room. The computer uses an external power supply which is required to power the CPU. The power supply was not taken. The computer has not been recovered after a thorough search. The computer was acquired on 07/28/09 under lease. The VA Police were notified and completed a Uniform Offense Report.

04/29/11:

There were no cameras in the area. Mental Health providers used this computer to administer the Mental Health Assistant program. The PC was basically functioning as a thin client, to access a local online test for patients. No information was stored on the local PC. The ISO investigated the remaining PC in the same room, used for the same purpose, and did not find any PII on it. Based on the fact that both computers were used for the same purpose, the ISO is confident there was no personally identifiable information (PII) on the stolen computer.

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE000000060761	Missing/Stolen Material (Non-Equipment)		VISN 16 Houston, TX		4/11/2011	4/26/2011	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
	4/11/2011	INC000000144445	N/A	N/A	N/A	210	
<p><b>Incident Summary</b></p> <p>At the end of the day on 04/08/11, a doctor locked and secured a room that contained an accordion folder with radiology order sheets with patients' information on them. Upon returning to work on 04/11/11, the doctor noticed the folder was missing and reported it to VA Police. VA Police notified the Information Security Officer (ISO). VA Police are currently investigating, creating a report, and determining what data was in the folder as well as who had keys to office, etc. They will provide VA Police report number once they have one.</p>							
<p><b>Incident Update</b></p> <p>04/15/11: Upon further investigation, 210 Veterans' information was lost including their names, full SSNs, dates of birth, and medical information. All 210 Veterans will be offered credit protection services.</p>							
<p><b>Resolution</b></p> <p>In addition to being in a locked office, all folders will now be placed in a locked file cabinet with limited key access to the file cabinet.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000060978	Mishandled/ Misused Electronic Information	VISN 16 Jackson, MS	4/14/2011		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
	4/14/2011	INC000000145254	N/A	N/A	N/A		

#### Incident Summary

A VA doctor used his personal camera to take pictures of patients and their procedures. He then loaded these pictures onto his personal laptop for transfer to a VA thumb drive. The photos included face shots and close up shots of procedures and wounds. This has been an ongoing practice that was just brought to the attention of the Information Security Officer (ISO) from a review of an Administrative Board investigation (ABI) report.

#### Incident Update

04/18/11:

There is no reason to believe that any images have been lost or accessed by anyone but the doctor. The doctor took the pictures on his camera, then down loaded them to his laptop, then copied them to his VA thumb drive and then loaded them onto his network drive. According to testimony for the ABI (which covered several areas besides this), he deleted the images after he transferred them. The physician took the photos to document his work. The information was not part of the patients' record and the physician did not get the patients' consent.

It is not yet known how many patients the doctor took pictures of. A request has been made to the facility Director to allow the ISO and IT personal access to the doctor's equipment pursuant to the memorandum from General Counsel on examination of employees private PCs and other devices. We are also requesting permission to examine his shared drive.

04/20/11:

Permission has not been granted yet to inspect the camera or the personal laptop but more will be known once those can be inspected. The ABI covered several issues beyond this one. Pertaining to this issue it was found that the doctor violated VA policy.

04/27/11:

The ISO has requested to be able to inspect the personal laptop, personal camera and network drive. Per direction from the Network ISO, those actions cannot be done until the Medical Center Director sends a request in writing to the Facility ISO. Currently the facility is undergoing a JCAHO visit as well as an ITOC visit along with another investigation. These various visits have made this incident a low priority for the Director; therefore the Facility ISO has not yet received the written request.

05/11/11:

The Director provided the memo authorizing the review of the doctor's personal equipment. The ISO will perform the review.

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE00000061210	Missing/Stolen Equipment		VISN 16 Biloxi, MS		4/19/2011	4/21/2011	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
	4/19/2011	INC000000146152	N/A	N/A	N/A		
<p><b>Incident Summary</b></p> <p>Computers and various components of the computers, as well as one personal digital assistant (PDA), were noted to be missing upon completion of a recent IT wall-to-wall inventory. The review was extensive and all avenues have been exhausted. The computers/peripherals/PDAs that are missing include 10 desktop PCs, 33 monitors, 13 printers, and 1 palm pilot.</p>							
<p><b>Incident Update</b></p> <p>04/21/11: The Chief Information Officer (CIO) stated that the desktops should not have any personally identifiable information (PII) or protected health information (PHI) stored on them.</p> <p><b>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.</b></p>							
<p><b>Resolution</b></p> <p>The 10 desktop PCs (not found during the inventory) were not encrypted because it is not customary to encrypt desktop PCs. They should not have had sensitive information on them.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000061346	Missing/Stolen Equipment	VISN 22 Long Beach, CA	4/20/2011		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
	4/20/2011	INC000000146262	N/A	N/A	N/A		

**Incident Summary**

A VA employee reported a missing workstation to the Information Security Officer (ISO) via email on 04/20/11 at 3:15 PM. The missing computer is a BioMed system, which ran the Varian Radiation Treatment Software. No VA sensitive information is stored on device. It is only used to control systems and communicate with Varian Servers.

The employee filed a VA Police report regarding the missing workstation. He believes that a few months after last year's inventory the computer had to be replaced. The employee checked with IT and BioMed to see if it could be located but it was not found.

There is no confidential patient information on the hard drive since all patient data is accessed through servers for CPRS, Vista and the department servers for Varian. A Report of Survey was prepared. The VA Police report is not completed yet.

**Incident Update**

04/21/11:

The VA Police report was completed. No data breach occurred. The missing computer was not used to store VA sensitive data.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000061529	Mishandled/ Misused Physical or Verbal Information	VISN 19 Cheyenne, WY	4/25/2011		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
	4/25/2011	INC000000146866	N/A	N/A	N/A	79	55

#### Incident Summary

A VA provider cleared out her office. She boxed up all of the documents in her office and placed them in a public hallway. She told a VA employee to take them from the hallway and throw everything away. A mail room clerk saw these boxes in the temporary construction dumpster located in a hallway outside of the pharmacy. One box was open. He looked inside the box and saw a patient's Personally Identifiable Information (PII) and Protected Health Information (PHI). He contacted the Privacy Officer (PO). The PO and another employee went through every box. There were complete medical records, progress notes, and notebooks full of patient information contained within the boxes. It is unclear as to how many Veterans' PII and PHI was in the boxes. The facility has not yet started to go through and log the individual patients' information found in the box.

#### Incident Update

04/25/11:

The temporary construction dumpster was in a hallway outside of the pharmacy and near the loading dock. It is accessible to the public. The PO is waiting for the reports of contact from the staff involved to determine how long the documents were in the dumpster. There is no security video in the area where the dumpster was sitting.

04/26/11:

The audiologist reports they were in the hallway for approximately one week before being taken to the dumpster. There were 127 patients' names and SSNs left unattended. All of the patients involved will be offered credit protection services.

05/02/11:

There were 134 individual patients' PII and PHI in the dumpster. Out of the 134 patients, 55 of the patients are deceased. There were many different documents on the same patients. The 79 patients will receive a letter offering credit protection services and the 55 deceased patients' next of kin (NOK) will receive NOK letters.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000061659	Mishandled/ Misused Physical or Verbal Information	VBA Montgomery, AL	4/27/2011		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
	4/27/2011	INC000000147368	N/A	N/A	N/A	897	

**Incident Summary**

VA Employees stored documents containing Veterans' full names and full SSNs in a desk drawer located in the front office and an unattended (unlocked) file cabinet in a Jobs Lab. The Vocational Rehabilitation and Employment (VRE) Services satellite location's front office desk drawer and the Jobs Lab file cabinet drawer are accessible to Veterans waiting to see their counselor or to use the Jobs Lab. The front office is periodically occupied by work-study students assigned to the office. The Jobs Lab may be unattended while the Veteran is using it.

**Incident Update**

04/28/11:

Because the Veterans' information was unsecured, 897 Veterans will receive a letter offering credit protection services.

05/02/11:

According to the Vocational Rehabilitation and Employment (VRE) Supervisor nothing, was missing from the desk or file cabinet. The Veterans' information was still at risk of exposure to unauthorized individuals, therefore 897 Veterans will still receive offers for credit protection services.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000061804	Mishandled/ Misused Electronic Information	VISN 19 Denver, CO	4/29/2011		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
	4/29/2011	INC000000147842	N/A	N/A	N/A		

#### Incident Summary

The Chief Medical Resident was questioned about how rotating residents communicated patient health information with other incoming residents. The Information Security Officer (ISO) and Privacy Officer (PO) were informed that they used a non-VHA email account off VHA campus to communicate medical health information.

#### Incident Update

05/02/11:

The medical attending physician has sent his explanation regarding the communication tool used by the residents as follows:

My understanding is that they use the ucdenver.edu webmail, a password protected email system for the university. Within that email structure, they have something akin to PKI - I think it is called Cisco encryption. We are instructing them to utilize that encryption function within that password protected email system. Further, we are instructing them to use minimal identifiers: never full SSN, never full name, usually a hybrid of part of last name and last 4 of the SSN. We want to be 100% certain that the correct patient is being identified but to also maximally limit the information contained therein.

With rotating house staff, it's critical that these handoffs occur and are effective ' poor handoffs present immediate threats to patient safety. Clearly, we must do all we can to safeguard patient privacy and confidentiality in doing so, the Shift Handoff Tool supports the above enterprise quite well and is the best electronic handoff tool across our hospitals.

05/11/11:

There is an academic affiliation between VA and UC. The residents see the patients at the VAMC. The residents use their own University of Colorado (UC) at Denver email accounts to share patient information. UC encryption is not as secure as VA Guardian Edge encryption.

Total number of Lost Blackberry Incidents	24
Total number of Internal Un-encrypted E-mail Incidents	77
Total number of Mis-Handling Incidents	95
Total number of Mis-Mailed Incidents	118
Total number of Mis-Mailed CMOP Incidents	7
Total number of IT Equipment Inventory Incidents	2
Total number of Missing/Stolen PC Incidents	1
Total number of Missing/Stolen Laptop Incidents	1