



---

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**  
**Feb 28 - Apr 3, 2011**

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000058877	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Chelmsford, MA	2/28/2011	3/25/2011	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
	2/28/2011	INC000000137143	N/A	N/A	N/A		1

#### Incident Summary

Patient A received the Medline Industries medical supply paperwork intended for Patient B. Patient B's name, address and type of medical supply were compromised. Patient A also received his medical supply labeled incorrectly. Syringes were labeled as Lancets. Patient A reported the incident to the medical center and replacements have been ordered. Chelmsford 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

02/28/11:  
Patient B will be sent a letter of notification.

**NOTE: There were a total of 16 Mis-Mailed CMOP incidents out of 7,578,912 total packages (11,151,652 total prescriptions) mailed out for this reporting period. Because of repetition, the other 15 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 packing error has been reported to Medline for investigation and corrective action.

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE000000058890	Mishandled/ Misused Physical or Verbal Information		VBA St Petersburg, FL		2/28/2011	3/10/2011	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
	2/28/2011	INC000000137189	N/A	N/A	N/A	1	
<b>Incident Summary</b>							
A document with Veteran A's name and SSN was faxed to an incorrect number. The individual who received the fax notified VA of the incident and returned it.							
<b>Incident Update</b>							
02/28/11: This was faxed to an individual outside of VA and included the Veteran's full name and full social security number. Veteran A will receive a letter offering credit protection services.							
<b>NOTE: There were a total of 107 Mis-Handling incidents this reporting period. Because of repetition the other 106 are not included in this report, but is 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>							
<b>Resolution</b>							
The employee who sent the fax was counseled. The credit protection letter was sent.							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000058907	Mishandled/ Misused Physical or Verbal Information	VBA San Diego, CA	2/28/2011		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
	2/28/2011	INC000000137260	N/A	N/A	N/A	1	
<b>Incident Summary</b>							
Veteran A was mailed a full copy of Veteran B's claim folder.							
<b>Incident Update</b>							
03/01/11: Veteran B's full social security number, date of birth, and medical information were disclosed. Veteran B will be offered credit protection services.							
<b>NOTE: There were a total of 129 Mis-Mailed incidents this reporting period. Because of repetition the other 128 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>							

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE000000058956	Mishandled/ Misused Physical or Verbal Information		VISN 11 Ann Arbor, MI		3/1/2011	3/8/2011	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
	3/1/2011	INC000000137391	N/A	N/A	N/A		
<p><b>Incident Summary</b></p> <p>A Human Resources (HR) employee placed VA sensitive documents in a plastic bin underneath her desk for future disposal. When she arrived at the office the next day, she discovered the plastic bin was emptied. The employee suspects the custodial staff emptied it. The HR employee contacted Facilities Management and the Information Security Officer (ISO). The missing documents have not been retrieved. The ISO confirmed with HR and the Privacy Officer (PO) that the appropriate mechanisms are in place to dispose of paper, and the practice to use temporary storage bins must stop. HR indicated they had problems in the past in regards to the VA shred bins not being emptied in a timely manner.</p>							
<p><b>Incident Update</b></p> <p>03/02/11: The estimate of individuals whose information was discarded is approximately 50 people, with a mix of VA employee's and outside applicants. However, there is no way to determine who those people are, unless the facility recovers the paperwork.</p> <p>03/08/11: Facilities Management checked and found that the trash from HR was already sent to the trash compactor by 10:00 AM that morning, and from there it was sent to a land fill. At the time of the incident, the PO stated that HR must discontinue the practice of using temporary storage bins (blue bins), as they have permanent disposal/recycle bins in their office space. Facilities Management also notified their staff not to remove any contents from the blue bins, but also told them the blue bins should not be used.</p>							
<p><b>Resolution</b></p> <p>The appropriate mechanisms to dispose of discarded documents containing personally identifiable information (PII) or protected health information (PHI) was discussed with the HR employees and they were instructed to notify their supervisor immediately if the designated shredder bins are too full to accept additional documents. HR was reminded to notify Facilities Management if the shredder bin is moved to a new location and the contractor who handles the removal of documents will be notified. The Facilities Management employee who emptied the recycle bins was counseled and a reminder memo was sent to all Facilities Management staff to only empty standard regulation trash containers.</p>							

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE000000059090	Non-VA Responsible/Non-Incident Upon Further Investigation		VISN 21 Manila, PI		3/3/2011	3/16/2011	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
	3/3/2011	INC000000137900	N/A	N/A	N/A		
<p><b>Incident Summary</b></p> <p>A Veteran who was interviewed by VBA for an appointment raised a concern on matters of privacy at VA Manila Outpatient Clinic (OPC). He said that privacy is not being fully implemented at the clinic. He alleged that he was at the clinic earlier, specifically, at the Patient Relations Assistant (PRA) area and that he saw some folders showing claims numbers. There were also some papers on top of the desks and tables, with information visible. Patients were being asked for their claim numbers, SSNs, and other personally identifiable information (PII) and could be overheard by others in the room.</p>							
<p><b>Incident Update</b></p> <p>03/04/11: The Information Security Officer (ISO) asked the Business Office Supervisor about the business processes regarding claims folders. Also, the ISO asked the Privacy Officer (PO) if there are local policy/guidelines in place about claims folders. The ISO and PO reminded all PRAs in public areas of the existing clean desk policy and implemented more frequent rounds on public areas.</p>							
<p><b>Resolution</b></p> <p>Staff was instructed to review the portion of Outpatient Clinic Policy 00-36 (Clean Desk Policy) which covers their responsibility to safeguard documents with sensitive information in unsecured areas. Employees must be conscientious of sensitive information on desktops and other work areas in the course of their daily work. Only sensitive information currently being used should be visible on the desktop and should be protected when dealing with customers. When not being used by staff, sensitive information is protected by covering or securing in a manner to prevent incidental disclosure. Documents on desk tops when unattended should be kept inside the drawer or left face-down.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000059445	Mishandled/ Misused Electronic Information	VISN 11 Ann Arbor, MI	3/10/2011	4/4/2011	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
	3/10/2011	INC000000138947	N/A	N/A	N/A		66

#### Incident Summary

On 02/03/11, the Eligibility Coordinator entered a backlog of approximately 2000 patients into the Enrollment Applications System (EAS), which is a national electronic VistA file that dates back to 2002. Some patients have made address corrections since the original application was completed. The application overwrote the current data and resulted in incorrect patient addresses in the system. This impacted the pharmacy prescription mailings and patients have been complaining that they have not received their medication. Pharmacy, Information Technology Staff, and others are currently reviewing the entire process to determine the extent of the patient information exposure and mismailed medications.

#### Incident Update

03/14/11:

The facility held a conference call on 03/11/11 to determine how many incorrect entries were made into the EAS. Only 1,367 patients had backlogged information entered. Not all of the patients' information was outdated and of those, only a portion had a letter or prescription mailed to them. The total number of patients with mismailed information is not known at this time; however it is currently believed to be between 150 and 300. The facility Privacy Officer is calling an emergency incident response meeting to investigate further. The facility is correcting the outdated information.

03/24/11:

Each service in the Medical Center compared all their mailings against the list of addresses that were entered incorrectly. They found the following mismailings:  
9 Pharmacy mismailings which included name and medication;  
40 appointment reminders which included name and appointment type;  
17 billing statements which included full name, address, diagnosis code and date of visit.

Sixty-six patients will receive a letter of notification.

#### Resolution

Eligibility/Enrollment staff have been retrained to follow the following sequence of events for data entry of each individual eligibility application (link to patient file, print online application, verify signature, file application) in order to prevent a back log of records requiring filing and recurrence of this address incident error.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000059721	Missing/Stolen Equipment	VISN 12 Milwaukee, WI	3/17/2011		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
	3/17/2011	INC000000140030	N/A	N/A	N/A		

#### Incident Summary

After an inventory of IT equipment, 3 laptops and 43 tower workstations were not located. The laptops did not contain any sensitive information and they are protected by Guardian Edge software. The search for the missing IT equipment is still ongoing and the IT staff does not believe these assets are out of VA control. The IT staff completed Reports of Survey for this equipment.

#### Incident Update

03/21/11:

The Information Security Officer (ISO) states that there are no technical controls preventing users from saving documents to the hard drives of workstations at the facility. All users are assigned a network storage drive and all users are instructed to save their documents on the network drive at new employee orientation. During additional computer training, all employees are instructed a second time to never save items to their hard drive. At this time, none of the items have been located. The following actions are being implemented immediately at the facility: All new workstations and laptops are being encrypted; a standardized Category Stock Number (CSN) is being used for all computer equipment; additional Equipment Inventory Listings (EILs) will be created to track equipment in specific sections; a weekly inventory by location will be implemented; and a tracking mechanism will be put in place for when computer items are moved.

**NOTE: There were a total of 6 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 5 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.**

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000060203	Mishandled/ Misused Electronic Information	VISN 11 Indianapolis, IN	3/30/2011		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
	3/30/2011	INC000000142334	N/A	N/A	N/A		184

#### Incident Summary

VA Neurosurgery Contract staff transmitted/stored VA patient personally identifiable information (PII) and protected health information (PHI) including name, last four digits of the SSN and diagnosis, to a non-VA website found at <http://www.editgrid.com>. The site is an on-line spreadsheet where users can save data and access it from any internet browser. The contract staff save VA PII/PHI in a spreadsheet, as a way to track their VA procedure schedule. A shared username/password is used by all contract staff to access the VA section of the website. The website provides no encryption (no https://).

The Information Security Officer (ISO) contacted the VA contract staff and instructed them to remove the VA PII/PHI from the site. They responded that they will do this immediately. The ISO also instructed the contract staff that transmitting/storing VA PII/PHI outside of VA was a violation of VA Policy and should never be done.

This issue is similar to the Google.docs that surfaced last year. Consideration should be given to block this URL at the VA gateway.

#### Incident Update

03/30/11:

VA NSOC blocked the gateway. One hundred eighty-four (184) patients will be sent a notification letter.

04/06/11:

The spreadsheet was on the web page since 2010. Ten (10) contract staff members and two (2) physicians that were not on the contract and were not authorized to see the data had access to the spreadsheet.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000060274	Mishandled/ Misused Physical or Verbal Information	VISN 12 North Chicago, IL	3/31/2011		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
	3/31/2011	INC000000142643	N/A	N/A	N/A	281	

**Incident Summary**

VA Police found one medium sized box of records, paper, and 5 1/4" floppy disks in corridor outside construction area in Building 134, 1st Floor. They took it into custody and turned it over to the Information Security Officer.

**Incident Update**

03/31/11:

The box contained 281 files. It was found just outside of an area where contractors were conducting demolition. The contractors set the box outside the area they were working and it was found by the police later. It is believed to have been there less than 24 hours.

04/06/11:

The files were old research documents containing personally identifiable information (PII) and protected health information (PHI). Prior to construction, the space was a cardiology clinic and it appears that the documents were inadvertently left behind when the occupants vacated.

04/07/11:

Two hundred and eighty one Veterans will receive a letter offering credit protection services.

Security Privacy Ticket Number	Incident Type		Organization		Date Opened	Date Closed	Risk Category
SPE000000060289	Missing/Stolen Equipment		VISN 18 Big Spring, TX		3/31/2011	4/1/2011	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
	3/31/2011	INC000000142710	N/A	N/A	N/A		
<b>Incident Summary</b>							
Two new laptops for contracting were reportedly received by the warehouse, processed and delivered to Information Technology (IT) staff. IT has one, but cannot locate the other. This piece of the equipment is not listed as being on the network nor does it show that it was ever inventoried by the IT staff. The Information Security Officer received a Report of Survey.							
<b>Incident Update</b>							
04/01/11: This laptop was never on the network or stored any sensitive information. It was not configured with VA software or encryption.							
<b>Resolution</b>							
This case was handed over to VA Police for investigation.							

Total number of Lost Blackberry Incidents	27
Total number of Internal Un-encrypted E-mail Incidents	95
Total number of Mis-Handling Incidents	107
Total number of Mis-Mailed Incidents	129
Total number of Mis-Mailed CMOP Incidents	16
Total number of IT Equipment Inventory Incidents	6
Total number of Missing/Stolen PC Incidents	3
Total number of Missing/Stolen Laptop Incidents	10 (6 encrypted)