

**Department of Veterans Affairs**



**Monthly Report to Congress  
On Data Incidents**

**August 30, 2010 – October 3, 2010**



October 7, 2010

**This Page Left Intentional Blank**

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0381107	Privacy	VBA St Paul, MN	8/30/10	9/9/10	40	Moderate	1
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
8/30/2010	INC000000109102	N/A		N/A		N/A	0

**Incident Summary**

Widow A received a notification letter that contained the discharge documents belonging to Veteran B. Veteran B's name, date of birth, dates of military service, and other information related to military service was disclosed. The social security number was not disclosed.

**Incident Update**

08/31/10:  
Veteran B will receive a letter offering credit protection services.

**NOTE: There were a total of 100 Mis-Mailed incidents this reporting period. Because of repetition, the other 99 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 received written counseling. The credit protection letter was sent.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0381280	Privacy	VHA CMOP LEAVENWORTH, KS	8/30/10	9/13/10	34	Moderate	0
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
8/30/2010	INC000000109173	N/A		N/A		N/A	1

**Incident Summary**

ChampVA Patient A received a prescription intended for ChampVA Patient B. Patient B's name and type of medication was compromised. Patient A reported the incident to "Meds by Mail" and a replacement was requested for Patient B. Leavenworth Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error. The CMOP employee will be counseled and retrained in proper packing procedures.

**Incident Update**

08/31/10:  
Patient B will receive a letter of notification.

**NOTE: There were a total of 33 Mis-Mailed CMOP incidents out of 7,144,426 total packages (10,510,547 total prescriptions) mailed out for this reporting period. Because of repetition, the other 32 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 notification letter was sent.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0381405	Missing/Stolen VA Resources	VISN 12 Madison, WI	8/30/10		13	Low	
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
8/30/2010	INC000000109238	8/30/2010		N/A		N/A	

**Incident Summary**

The Facility ISO (FISO) was notified that a PC/workstation was missing from the Rockford Clinic. The VA Police Department was notified. The investigation is continuing.

**Incident Update**

08/31/10:

The PC was discovered missing by a Medical Technician when he arrived at work on 08/30/10. It was last seen on 08/27/10. It was used to access VistA and CPRS. There was no PII or PHI stored on the PC. The lab was not locked and there were no cameras in the area. There are no signs of forced entry into the building and there are no other items known to be missing at this time. Staff at the clinic have been interviewed and it has been determined that the building was secured at the end of the day on Friday. There were staff working in the registration area on Saturday, 08/28/10 and they reported nothing out of the ordinary, and once again, the building was secured upon their departure. There were seven employees working on Saturday at the Rockford Clinic. All seven were interviewed by the Madison VA Police as part of the ongoing investigation and none of them had occasion to go back into the lab on Saturday. The CPU in question was not visible from the registration area or from the hallway.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0381478	Privacy	VISN 07 Columbia, SC	8/30/10	10/6/10	18	Moderate	1
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
8/30/2010	INC000000109284	N/A		N/A		N/A	0

**Incident Summary**

On 08/29/10, an Emergency Room employee handed Veteran B's patient profile/medication order to Veteran A in Emergency Room. The error was discovered when Veteran B arrived at the Pharmacy pickup window to pick up his medication and there was no order. Veteran B presented a printout of active and pending medications to the Pharmacy employee. Upon review of the paperwork, it was discovered that Veteran A had been given the wrong Patient profile paperwork. The Pharmacy Supervisor notified Veteran A and the Privacy Officer of the incident by phone, Veteran A is aware that he has wrong medication order, no incorrect medication was issued to Veteran A. The information disclosed was Veteran B's name, date of birth, social security number, the name of active medications, pending medications, non-VA medications, provider's name and follow up instructions.

**Incident Update**

08/31/10:

Veteran B will receive a letter offering credit protection services

**NOTE: There were a total of 60 Mis-Handling incidents this reporting period. Because of repetition, the other 59 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 credit monitoring letter was sent.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0381946	IT Equipment Inventory	VISN 07 Tuscaloosa, AL	8/31/10	9/22/10	8	Low	
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
8/31/2010	INC000000109413	N/A		N/A		N/A	

#### Incident Summary

The CIO notified the ISO that six workstations were unaccounted during the end-of-year inventory. Three of the workstations had been previously turned-in and were believed to be in the warehouse. The remaining three workstations were new leased PCs and never deployed. A Report of Survey was generated and VA Police initiated the Uniformed Officer's Report. None of the workstations contained personally identifiable information (PII) and/or protected health information (PHI).

#### Incident Update

**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.**

#### Resolution

A Report of Survey was generated and VA Police initiated the Uniformed Officer's Report. None of the workstations contained personally identifiable information (PII) and/or protected health information (PHI).

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0384414	Privacy	VBA Boston, MA	9/7/10	9/24/10	34	High	3,936
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
9/7/2010	INC000000110266	N/A		N/A		N/A	30

#### Incident Summary

It was reported that on 08/25/10, 6,299 out of the 69,366 "Benefit Summary" letters intended for Veterans and non Veterans in the state of Massachusetts were mailed to incorrect addresses. The letters contain Veterans' and Non-Veterans' benefit information to include the claim number which, in some instances, may be the Veterans' full social security number (SSN).

#### Incident Update

09/07/10:

VBA has determined that 3,913 of the 6,299 letters contained the full SSN and 2,386 contained the VBA claim number. The incident occurred as a result of a programming error. The vendor (Performance Analysis & Integrity) merged Veteran data with an old address data base which caused the letters to be mailed to the incorrect addresses. To compound the issue, the names of some of the Veterans were not visible in the window of the envelope resulting in some of the letters being opened by third party individuals at the address. The incident was discovered on 09/01/10 when a civilian notified the Boston VBA Regional Office of the mismailing. Analysis confirmed that a mass mismailing occurred.

09/09/10:

The final count of unique Veterans whose SSN was exposed is 3,936. There was an additional 30 SSNs of deceased Veterans exposed. Therefore 3936 Veterans will receive credit protection letters and 30 Survivors will receive next-of-kin notification letters.

09/23/10:

The Office of Risk Management and Incident Response advised that the 3,936 letters with Veterans' SSNs were potential breaches of privacy that required VA to offer credit monitoring. The 30 letters to survivors that included the deceased Veteran's SSN required next-of-kin letters. A letter explaining the incident and offering VA-sponsored credit protection services was released to the 3,936 affected Veterans. The next-of-kin letter was sent to 30 survivors. Hines ITC generated and mailed the letters. The mailings included a copy of the original (misdirected) Benefits Summary Letter.

#### Resolution

The notification and credit monitoring letters have been mailed.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0386987	Missing/Stolen VA Resources	VISN 10 Cleveland, OH	9/13/10	9/17/10	32	Moderate	0
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
9/13/2010	INC000000111195	9/13/2010		N/A		N/A	332

#### Incident Summary

A user reported her PC workstation is missing and was possibly stolen from her work area. The PC workstation was in an office that is not secured by a physical door and uses only a curtain for privacy. The user has not yet been interviewed about possible PII or PHI on that workstation. The VA Police Services has been notified and are taking the report at this time from IT staff.

#### Incident Update

09/15/10:

According to the ISO, the workstation contained Microsoft Excel spreadsheets with patient appointment data that included the last name and last 4 of SSN of up to 175 Veterans. The workstation did not have any security cables in place. VA Police Service is investigating the theft.

09/16/10:

The user has been mandated to take Information Security Awareness Training again within 30 days. The user has been instructed and shown how to save all documents to the network drive. The 175 Veterans will receive a notification letter.

09/29/10:

After further review, there are 332 names and not 175 that the user estimated.

#### Resolution

The notification letters have been sent.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0387594	Privacy	VISN 22 Loma Linda, CA	9/14/10		38	High	106
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
9/14/2010	INC000000111425	N/A		N/A		N/A	0

#### Incident Summary

The Office of Corporate Compliance and Loma Linda University (LLU) Adventist Health Science Center sent a letter to the VA Quality Management Office to say that they were in possession of several patients' records from the VA Medical Center. The records were found by a security officer on or about 07/30/10. It is believed that the records were in the possession of a resident physician in the University Medical Program. Apparently, the resident was in the process of moving his belongings. The box was left on the curb near the residence. The box of documents, compensation and pension exams, X-Ray and MRI films were taken to the compliance office and kept there until someone at the VA staff retrieved the box. The records contained names, home addresses, dates of birth, PHI and the social security numbers of 116 Veterans.

#### Incident Update

09/14/10:

The doctor was a Fee Base Doctor and is no longer employed with VA. He was employed from 01/09 to 07/10. The ISO has the records in his possession. A team was assembled to investigate this matter. After further investigation by the ISO, it was determined that there were 106 records potentially compromised. 106 Veterans will receive a letter offering credit protection services.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0388130	Missing/Stolen VA Resources	VISN 01 West Haven, CT	9/15/10	9/17/10	42	Moderate	
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
9/15/2010	INC000000111648	N/A		N/A		N/A	

**Incident Summary**

It was reported that two CPUs were missing from rooms in Primary Care. Only the CPUs were taken. The monitors, mice and keyboards were left behind.

**Incident Update**

09/16/10:

According to the ISO, the users stated that no PII/PHI was stored on workstations. There were no security cables securing the CPUs. A VA Police report was filed. The Police reviewed the security tapes in the area and nothing was found. The local police and Pawn Shops were notified of the theft.

09/27/10

The two CPUs were in offices in the Primary Care area. The offices are usually locked but may have been opened for housekeeping. Both CPUs were used to access CPRS. They were discovered missing by the RN when she reported to duty. The phone in one of the offices was also taken. The VA Police have closed their investigation.

**Resolution**

A reasonable search was conducted and nothing was found.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0391203	Privacy	RCS Lakewood	9/22/10		39	Moderate	
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
9/22/2010	INC000000112826	N/A		9/22/2010	Pending	Pending	

#### Incident Summary

Veteran A contacted the Albuquerque Vet Center this morning from their current location at Fort Benning, GA, where Veteran A was scheduled to deploy on active duty to Afghanistan as a member of the U.S. Army. Veteran A consulted with a physician who informed Veteran A of not being eligible for deployment due primarily to the content of a progress note recorded earlier in Veteran A's treatment at the Vet Center. A copy of the progress notes and specific traumatic events as noted in the military history for Veteran A per Vet Center intake protocol. Veteran A indicated a signed release of information was not obtained allowing the Department of Defense or the Department of the Army to access the treatment records at the Readjustment Counseling Services of the VA, nor has this readjustment counseling therapist received any request to disclose such information from any source. The veteran was extremely upset at this disclosure.

#### Incident Update

10/06/10:

According to ISO, the Doctor stated they accessed the information via DOD AHLTA (Armed Forces Health Longitudinal Technology Application) system that connects to VA VistA system, but according ISO the DOD did not access the Vet Center's system, this does not rule out other methods. Based on review of RCSnet no breach was identified and after review of accounts all accounts are appropriately assigned. RCS staff was able to obtain permission to access the DOD system and is in the process of scheduling a time to go to Ft. Benning to see exactly how the doctor saw the information and to determine if a HIPAA violation occurred or if there is a computer system issue between the VA VistA system and the VET Center's system.

<b>VA-NSOC Incident Number</b>	<b>Incident Type</b>	<b>Organization</b>	<b>Date Opened</b>	<b>Date Closed</b>	<b>FERET Score</b>	<b>Risk Category</b>	<b>No. Of Credit Monitoring</b>
VANSOC0391477	Missing/Stolen VA Resources	VISN 11 Ann Arbor, MI	9/22/10		26	Low	
<b>Date US-CERT Notified</b>	<b>US-CERT Case Number</b>	<b>Date Privacy Notified</b>	<b>(Old)PVTS Number</b>	<b>Date OIG Notified</b>	<b>Accepted by OIG</b>	<b>OIG Case Number</b>	<b>No. of Loss Notifications</b>
9/22/2010	INC000000112905	N/A		N/A		N/A	

**Incident Summary**

A VA laptop used for dosimeter readings for x-ray exposure was shipped to the vendor on 09/09/10 for maintenance. The vendor responded back stating the hard drive was missing.

**Incident Update**

09/22/10:

The ISO contacted the radiation health specialist to determine the type of data stored on the device. The data stored is the level of radiation exposure. Once a badge is read, the measurement is entered separately into VISTA. The laptop was not encrypted, but it was secured when not in use and did not leave the facility.

09/23/10:

According to the staff, there is no PII/PHI on the laptop. It was used for dosimeter reading of radiology staff badges on radiation exposure. This is a standalone device that does not need to connect to the network. According to the ISO, the laptop was used infrequently and the last known use was 3-4 months ago. Therefore, it does not have the standard active directory setup to determine the last network account to use the device. When not in use, it is/was locked in a secure room at the facility.

Total number of lost Blackberry incidents	14
Total number of internal un-encrypted e-mail incidents	97
Total number of Mis-Handling Incidents	60
Total number of Mis-Mailed Incidents	100
Total number of Mis-Mailed CMOP Incidents	33
Total number of IT Equipment Inventory Incidents	6
Total number of Missing/Stolen PC Incidents	3
Total number of Missing/Stolen Laptop Incidents	10 (5 encrypted)