



DEPARTMENT OF VETERANS AFFAIRS
Information Technology Field Operations
Field Security Operations
Network and Security Operations Center (NSOC)



Monthly Report to Congress of Data Breaches

Apr 5 - May 2, 2010

WARNING: This document is FOR OFFICIAL USE ONLY. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). This document is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel without prior approval of the Veterans Affairs Chief Information Officer. Where appropriate, U.S. person identities have been removed. Should you have a requirement for particular U.S. person identity information, contact the VA-NSOC. No portion of this report should be furnished to the media, either in written or verbal form.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0315078	Privacy	VISN 07 Augusta, GA	4/5/10	4/22/10	35	High	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
4/5/2010	INC000000086062	N/A		N/A		N/A	0

Incident Summary

Patient A was given the lab specimen order for Patient B. Patient A took the order home with him before returning to report that the order was not his. Patient A returned the specimen order to the Downtown Division lab staff. The document contains Patient B's full name, date of birth, full SSN, sex, physician, test, and collection sample name.

Incident Update

04/06/10:

Patient B will receive a letter offering credit protection services.

NOTE: There were a total of 104 Mis-Handling incidents this reporting period. Because of repetition the other 103 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

A signed, redacted credit protection letter is attached. The Downtown Division Laboratory staff were made aware of incident and corrective action was taken.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0316500	IT Equipment Inventory	VISN 10 Chillicothe, OH	4/7/10	5/12/10	14	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
4/7/2010	INC000000086430	N/A		N/A		N/A	

Incident Summary

The local Chief Information Office's annual Equipment Inventory Listing (EIL) inventory concluded with 55 items unaccounted for, including 1 Air Fortress Encryption Device, 2 Barcode Readers, 7 Barcode Scanners, 1 laptop cart, 1 CDROM rewritable disk drive, 7 computer workstations, 2 laptops, 1 Duplex Card Scanner, 1 Flatbed Scanner, 5 Monitors, 19 Pagers, 1 Videoconference Polycom, 6 Printers, and 1 UPS.

Incident Update

04/09/10

The missing PCs were not encrypted but were not used for storing patient data. In addition, employees are instructed to:

A.) Not save unnecessary patient data; and

B.) Not save any information at all on the local C: drive.

The systems are setup so that all Microsoft products (Microsoft Office) save to the network drives by default. The 2 laptops were BCMA (Bar Code Medication Administration) laptops and were also not encrypted. The other devices were not storage capable.

NOTE: There were a total of 8 IT Equipment Inventory Incidents this reporting period. Because of repetition the other 7 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Resolution

The Reports of Survey have been submitted.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0316509	Missing/Stolen VA Resources	VISN 16 Houston, TX	4/7/10	5/16/10	26	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
4/7/2010	INC000000086431	N/A		N/A		N/A	

Incident Summary

A standard PC workstation was reported by a VA nurse to be missing from a Mental Health group room used by both staff and patients for various meetings and group sessions. It does not store data, but allows the user to connect to the servers where the data resides using log-in credentials. The group room is used by all the clinical staff in the area and was left unlocked. The VA nurse reported it to the VA Police who then notified OI&T. The computer information (serial number, etc.) was given to the VA Police who are investigating.

Incident Update

05/14/10:

The ISO confirmed with VA Police staff that the VA Police closed their investigation and transferred the case to the VA Detective for further investigation.

Resolution

The ISO has requested the ticket to be closed since there is no indication this PC will be recovered.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0316557	Privacy	VBA Buffalo, NY	4/7/10	4/12/10		Low	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
4/7/2010	INC000000086450	N/A		N/A		N/A	0

Incident Summary

Veteran A received documents intended for Veteran B in the same envelope with his letter. The information included Veteran B's name, address, and social security number.

Incident Update

04/08/10

Veteran B will receive a letter offering credit protection services.

NOTE: There were a total of 96 Mis-Mailed incidents this reporting period. Because of repetition the other 95 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 credit protection offer letter has been sent.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0317032	Privacy	VHA CMOP DALLAS, TX	4/8/10	4/23/10	36	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
4/8/2010	INC000000086562	N/A		N/A		N/A	1

Incident Summary

Patient A received a Medline Industries medical supply intended for Patient B. Patient B's name and type of medical supply was compromised. Patient A reported the incident to the medical center and a replacement has been requested for Patient B. The Dallas Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a Medline packing error, and it has been reported to Medline for investigation and corrective action.

Incident Update

04/09/10
Patient B will receive a letter of notification.

NOTE: There were a total of 21 Mis-Mailed CMOP incidents out of 5,346,344 total packages (8,085,271 total prescriptions) mailed out for this reporting period. Because of repetition the other 20 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 has been sent.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0317603	Privacy	VISN 01 White River Junction, VT	4/9/10		35	Moderate	172
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
4/9/2010	INC000000086796	N/A		N/A		N/A	20

Incident Summary

Two hundred and three Veteran photos were found on the VA loading dock by the VA police. Of these photos 172 have the Veterans' names and full social security number marked on the photo. Nine have the Veterans' names and the last 4 digits of the social security numbers. Nine photos only have the Veterans' names, and 2 photos have only the last names marked. The remaining photos are duplicates.

Incident Update

04/09/10:

The photos were found in a small gray metal box which is currently in the Privacy Officer's possession. They were on the loading dock for up to 6 hours. There are no security cameras on the loading dock.

04/13/10:

The Privacy Officer was unable to determine how the photos arrived on the loading dock. The Privacy Officer will write a Medical Center Memo to provide the facility with a process for addressing records management and security prior to relocation of space.

04/28/10:

One hundred seventy-two (172) Veterans will receive a letter offering credit protection services. Twenty (20) Veterans will receive a letter of notification.

05/11/10:

A VA staff member on the inpatient ward was responsible for the breach and was educated on records management and control of sensitive data. All facility staff who was involved with the documents was educated on good records management methods, as well as how to effectively safeguard patient information. A new policy implemented during clinical relocations is to have the Privacy Officer and Records Manager meet with the section one month prior to the move to ensure that any records that are past the disposition period are properly destroyed and that the Health Information will be boxed and stored in accordance with VHA privacy standards.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0318008	Missing/Stolen VA Resources	VISN 23 Iowa City, IA	4/10/10		47	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
4/10/2010	INC000000086942	N/A		N/A		N/A	

Incident Summary

A VA Research employee reported that a new VA computer was stolen from an animal research project's collaborative study lab site from the Iowa State University campus. The PC was taken directly from the box it was shipped in and was never connected to the network. It was not encrypted and had no PII or PHI. The City Police and VA Police have been notified. The exact time of the theft is unknown at this time.

Incident Update

04/27/10:

The ISO is still waiting for the final Police reports.

05/07/10:

The laptop was determined to be missing by Research personnel. It was missing from a joint Iowa State University and VA Research site in the central part of the state and was not actually at a VA facility. They were getting ready to deploy the PC. The rest of the system was not touched.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0318440	Privacy	VISN 20 Walla Walla, WA	4/12/10	4/17/10	31	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
4/12/2010	INC000000087080	N/A		N/A		N/A	60

Incident Summary

Paper documents containing patient behavioral health and personal information were left in a VA conference room following a mental health group counseling meeting.

Incident Update

04/14/10:

Communication with the ISO verified that the medical information was exposed from a Wednesday to a Friday in a room that was very accessible to staff, patients and visitors. The SSN and DOB were not exposed.

04/14/10:

Sixty (60) Veterans will receive a letter of notification.

05/18/10:

Some of the documents appeared to be original DD214s and they are being scanned in and will be sent back to the Veterans.

Resolution

The notification letters were mailed.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0319127	Privacy	VISN 11 Indianapolis, IN	4/13/10		33	High	121
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
4/13/2010	INC000000087430	N/A		N/A		N/A	60

Incident Summary

At approximately 2:00PM on 04/13/10, an Industrial Hygienist from the facility Safety Office came to a conference room in HIMS where the facility Privacy Group was meeting. He stated that he was checking dumpsters near a loading dock on the West side of the facility and tore open a dark plastic bag which was knotted on top. The contents revealed patient information. The Privacy Officer (PO) immediately followed him to the site where they secured the barrel. The PO called Assistant Chief of EMS and the dumpster was secured. The contents will be inventoried starting tomorrow. Many of the sheets of paper were stuck together from rain but were clearly readable. The medical records of numerous patients along with their sensitive information were found in the bag. The medical records contained names, full social security numbers, and PHI.

Incident Update

4/16/10:

The material in the bag has been inventoried by medical center staff. All the documents (i.e., patient history, lab results, progress notes, radiology reports) appear to have been generated on one ward (7A North) which is a 30 bed unit. The information is for a 2 week period of time from approximately December 29, 2009 through January 7, 2010; identifying 182 individuals.

This trash bag was contained in a 55-gallon recycling bin that would normally be emptied into a larger dumpster for removal by a recycling contractor. The Housekeeping Aid, who is assigned to that area, identified the bin as having unusual contents, alerted his supervisor, and then set the bin aside. Subsequently, the medical center's Industrial Hygienist, on routine surveillance rounds, looked into the bin, became concerned, and alerted the Assistant Chief of Environmental Management. It is against protocol and training for documents to be handled in this fashion. The medical center destroys approximately 10 tons of documents each month.

All trash containers on 7A North are being looked at today to ensure this is a one-time failure and not a pattern. A review team has been established to determine any other facts relevant to this situation, if possible what systems failures led to this point, what if any corrective actions need to be taken, and whether any disciplinary actions are indicated. The review findings will be reported to the Network Director by April 20, 2010.

04/20/10:

Of the 182 individuals, the following is a breakdown:

1. 121 displayed full SSN, DOB and age
2. 60 displayed partial SSN
3. 1 did not display an SSN (Employee)
4. All were patients except one
5. All but one displayed medical information. (Employee is exception)
6. One displayed financial and personal information (Employee)
7. No patients displayed home address or phone numbers

4/20/10:

One hundred and twenty one (121) patients will receive a letter offering credit protection services and sixty (60) patients will receive letters of notification.

05/13/10:

The majority of the letters have gone out. The PO has approximately 10 letters for deceased patients that he is trying to finalize.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0319741	Investigation	VISN 11 Ann Arbor, MI	4/14/10	5/12/10	19	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
4/14/2010	INC000000087512	N/A		N/A		N/A	

Incident Summary

A VA employee from beneficiary travel noticed that recent patient address changes which occurred multiple times within the last couple months may be related to fraudulent activity. This activity has been reported to the VA OIG by VA Police. The VA police approached the ISO to determine if there were any methods available to track this activity. Upon investigating the patient record, the ISO noted the record was not marked as sensitive, therefore that status was changed to capture future activity.

Incident Update

04/15/10:

According to the Facility's Chief of Police, the OIG is conducting a full investigation into this matter. Until they have completed their investigation, there will not be an official police report. Several of the addresses have been identified as businesses and, in one case, the office of a state representative. This case is under Investigation.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0320255	Missing/Stolen VA Resources	VISN 04 Philadelphia, PA	4/15/10		18	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
4/15/2010	INC000000087657	N/A		N/A		N/A	

Incident Summary

A leased laptop used for sleep study research was found missing. The device was secured in place by a cable lock. The last known location was on Thursday, 04/08/10. A resident reports that he noticed the laptop was not present on Monday or Tuesday, 04/12/10 and 4/13/10. The unencrypted device does not contain PII or PHI data, but does contain study ID and raw data of residents. The device is not connected to the VA network and the network interface is disabled. The room location is normally open. The cable locking device appears to have been tampered with. The VA police were notified and the officer arrived to the location and secured the locking cable. The ISO is awaiting confirmation of the make, model and serial number from the research coordinator.

Incident Update

04/27/10:

The VA police detective in charge of the investigation will be starting interviews this week. The ISO has been collecting employee information, dates and work times.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0322429	Privacy	VISN 19 Cheyenne, WY	4/20/10	4/28/10	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
4/20/2010	INC000000088408	N/A		N/A		N/A	175

Incident Summary

A VA employee printed a Prosthetic open/pending suspense list and accidentally mailed it to Patient A. The list contained 175 Veterans' names and partial social security numbers.

Incident Update

04/21/10:

The one hundred seventy-five (175) patients will receive a letter of notification.

04/26/10:

The PO spoke to the supervisor of Prosthetics and gave the supervisor a copy of the list of patients that was mailed to Patient A. The supervisor stated there is no way to determine who mailed the list out. The PO suggested education for all of the employees who work in the area.

Resolution

The supervisor is providing education to entire staff as she is not sure who sent the list patients names and last four to Patient A. The notification letters were sent.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0323048	Missing/Stolen VA Resources	VISN 09 Mountain Home, TN	4/21/10		29	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
4/21/2010	INC000000088575	N/A		N/A		N/A	

Incident Summary

A VA physician reported a laptop missing from Audiology and Speech Pathology secured computer lab area. This laptop is a specialized research laptop that is "locked down" to only allow the software for the research to be utilized by Veterans. This laptop does not connect to the network and contains no PII per audiology, but is not encrypted.

Incident Update

05/12/10:

The laptop was used for Audiology research and was purchased with grant money. There was no PII or PHI stored on the laptop. It was never connected to the network and was password protected. The area has been searched and all staff was questioned.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0323068	Improper Usage	VISN 07 Decatur, GA	4/21/10		39	Moderate	278
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
4/21/2010	INC000000088588	N/A		4/22/2010	Pending	Pending	0

Incident Summary

A contract employee may have copied patient data and/or sent patient data to herself via email. This employee was terminated today but she sent an email to the Chief of HAS stating that she had data that she plans to send to the OIG or a whistleblower group if her employment conditions were not met. The ISO was unable to verify if data was sent out of the facility via email until the exchange account is audited. Neither the ISO nor the Privacy Officer was able to speak to the employee before they were terminated.

Incident Update

04/22/10:

This incident has been reported to OIG for further review.

04/26/10:

The supervisor stated that the contract employee did not have access to the data that was sent in the email and that only one other person had access to the data besides the supervisor. There is an interview scheduled on April 26th with the other employee who had access to the data today concerning this incident.

05/10/10:

The former employee could have printed the information and taken a hard copy. IT is checking to see if SANCTUARY was deployed to the system. The file had 278 patients listed. The 278 patients whose name and SSN were in the file and on the list 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
VANSOC0324809	Privacy	VBA Buffalo, NY	4/26/10	4/29/10	52	High	71
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
4/26/2010	INC000000089178	N/A		N/A		N/A	0

Incident Summary

Veteran A is concerned that she mistakenly received some sensitive information pertaining to more than 70 Veterans, including names and social security numbers via mail from the VA.

Incident Update

04/28/10:

The seventy (70) Veterans and the 1 patient will receive a letter offering credit protection services.

04/29/10:

Credit monitoring has been requested and approved for Veteran A. In addition, the PO was able to locate 13 Veterans out of the 70 in SHARE and obtain addresses for them. Credit monitoring has been requested for the 13 Veterans.

05/13/10:

The orders, which are for the other Veterans and are included in Veteran A's C file (that is located in this office), are from the 1980s. The PO entered the social security numbers and names for all 71 Veterans in the data base in an attempt to find addresses for them. The PO found addresses for 13 of the Veterans who are currently receiving benefits, or have received benefits at one time. It is not possible to locate addresses for the other Veterans as they have never received benefits and are not in this database. The copies never left the hands of Veteran A, and only VA employees have had access to Veteran A's file. Veteran A returned the copies to VA.

Resolution

The credit protection letters were sent.

Total number of lost Blackberry incidents	22
Total number of internal un-encrypted e-mail incidents	79
Total number of Mis-Handling Incidents	104
Total number of Mis-Mailed Incidents	96
Total number of Mis-Mailed CMOP Incidents	21
Total number of IT Equipment Inventory Incidents	8
Total number of Missing/Stolen PC Incidents	3
Total number of Missing/Stolen Laptop Incidents	6 (4 encrypted)

WARNING: This document is FOR OFFICIAL USE ONLY. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). This document is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel without prior approval of the Veterans Affairs Chief Information Officer. Where appropriate, U.S. person identities have been removed. Should you have a requirement for particular U.S. person identity information, contact the VA-NSOC. No portion of this report should be furnished to the media, either in written or verbal form.