Department of Veterans Affairs

Monthly Report to Congress On Data Incidents

Nov 1 – 28, 2010

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000054107	Mishandled/ Misused Electronic Information	VISN 01 Manchester, NH	11/1/2010	12/7/2010		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
VANSOC0410256	11/1/2010	INC000000119907	N/A	N/A	N/A	1	0

Incident Summary

The Request for Information (ROI) clerk printed out records for Veteran A which contained scanned documents for Veteran B. The documents contained Veteran B's name, DOB and partial SSN. Veteran A returned the documents to the ROI clerk.

Incident Update

11/02/10:
Veteran B will receive a letter offering credit protection services.

NOTE: There were a total of 64 Mis-Handling incidents this reporting period. Because of repetition, the other 63 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 protection letter was mailed.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000054114	Missing/Stolen Equipment	VISN 17 Temple, TX	11/1/2010	11/27/2010		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
VANSOC0410294	11/1/2010	INC000000119928	N/A	N/A	N/A		

Incident Summary

Following an IT inventory, two VA Police reports were filed for missing and unaccounted for IT equipment. The first Police report was for the Waco facility in which 4 desktop computers and 9 monitors were reported missing. The second Police report was for the Temple facility in which 43 computers, 3 laptops (encrypted), 25 monitors, 10 printers, 1 switch, and 2 disk drives were reported missing. Per the facility Chief Information Officer (CIO), the desktop computers listed on the Report of Surveys (ROS) were most likely processed for turn-in.

Incident Update

11/02/10:
OI&T has local IT Standard Operating Procedures for processing turn-in equipment that includes removal of data on the hard drive, removal of the hard drive, and processing the hard drives for destruction in accordance with Intelligent Decisions, a national contractor. This process is done for every device removed from service. The facility CIO stated he is highly confident the process was followed for the missing devices noted on the ROS. The facility CIO stated the failure on the part of OI&T staff is the inability to produce the documentation showing the equipment for turn in was processed. The facility CIO stated OI&T designated one staff to be dedicated to the process for equipment turn in and currently has a full time OI&T Asset Manager responsible for tracking all OI&T equipment. Both the OI&T Asset Manager and the OI&T Chief, Systems and Networking Section assured the ISO the computer desktops on the ROS do not contain sensitive information. The OI&T Chief, Systems and Networking Section further stated that based on the workstation image for that time frame, it did not allow users to save data locally to the computer workstations. The OI&T Asset Manager stated the two disk drives, not accounted for and listed on the ROS, are believed to be installed in the HP Network Storage Array (NSA) part of the VistA system.

NOTE: There were a total of 4 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 3 are not included in this report, but is included in the "IT Equipment Inventory Incidents" count at the end of this report.

Resolution

The recently hired IT Assets Manager created a database to help track and cross reference multiple data sources including, but not limited to, OI&T ROS from FY 2009, 2010, and 2011. The two disk drives were confirmed to be part of the HP NSA and are not missing.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000054148	Mishandled/ Misused Physical or Verbal Information	VBA Muskogee, OK	11/2/2010	11/18/2010		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
VANSOC0410724	11/2/2010	INC000000120103	N/A	N/A	N/A	1	0

Incident Summary

A letter addressed to Veteran A dated 10/13/10 was received by Veteran B and returned to the Regional Office. The misdirected correspondence was received in the same envelope as a letter addressed to Veteran B. The letter contained Veteran A's name, social security number, address and medical conditions.

Incident Update

11/03/10:
Veteran A will receive a letter offering credit protection services.

NOTE: There were a total of 78 Mis-Mailed incidents this reporting period. Because of repetition, the other 77 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 monitoring letter has been sent.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000054266	Missing/Stolen Material (Non-Equipment)	VISN 15 Kansas City, MO	11/3/2010	11/17/2010		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
VANSOC0411867	11/3/2010	INC000000120414	N/A	N/A	N/A		

Incident Summary

A VA Pathology employee contacted the VA Police to report that a VA desktop computer was missing. The computer was located in the Pathology lab and used by 12 employees.

Incident Update

11/04/10:
According to the users and the Automated Data Processing Application Coordinator (ADPACs), the system was only used to enter lab results into VistA and no sensitive information was stored locally. The VA Police are investigating the incident, interviewing the users, and there is a uniform offense report (UOR) on file. The computer was located in the lab which is occupied 24 hours a day. Nothing else was missing. There are no cameras in the area. IRM stated that they were not able to "ping" the desktop computer and that it was disconnected from the network approximately seven days ago.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000054306	Mishandled/ Misused Physical or Verbal Information	VISN 17 Dallas, TX	11/4/2010	11/30/2010		High

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
VANSOC0412344	11/4/2010	INC000000120527	N/A	N/A	N/A		140

Incident Summary

A VA Attorney discovered names, partial social security numbers and treatment locations of approximately 140 Veterans inter-mingled with other paperwork. The Business Office employee who submitted the EEOC claim had attempted to redact the names of the individuals, although they were still legible. The information was disclosed to the EEOC in Dallas.

Incident Update

11/04/10:
The EEOC employees do not have the authorization to review the information. One hundred - forty (140) Veterans will receive a letter of notification.

Resolution

The notification letter was sent out on 11/30/10.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000054479	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Dallas, TX	11/8/2010			High

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
VANSOC0414077	11/8/2010	INC000000121333	N/A	N/A	N/A	0	1

Incident Summary

Patient A received a prescription intended for Patient B. Patient B's name and type of medication was compromised. The investigation reveals that this was a CMOP packing error. The employee has been counseled and retrained.

Incident Update

11/09/10:
Patient A will receive a notification letter.

NOTE: There were a total of 5 Mis-Mailed CMOP incidents out of 5,586,204 total packages (8,236,621 total prescriptions) mailed out for this reporting period. Because of repetition, the other 4 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.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000054613	Mishandled/ Misused Physical or Verbal Information	VBA St Paul, MN	11/10/2010	11/16/2010		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
VANSOC0415351	11/10/2010	N/A	N/A	N/A	N/A	57	

Incident Summary

The St. Paul Veterans Service Center (VSC) was informed of a Privacy Act violation by a federal fiduciary. The fiduciary inappropriately shared 58 VA guardianship files with another federal fiduciary who was not authorized to view or receive the Veterans' claims related material. The information disclosed included the full names and SSNs of the Veterans.

Incident Update

11/10/10:
Fifty - Eight (58) Veterans will receive a letter offering credit protection services.

11/16/10:
The number of Veterans affected was changed to 57 due to a duplicate listing.

Resolution

Additional training was provided to the fiduciary.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000054736	Missing/Stolen Equipment	VISN 22 Los Angeles, CA	11/15/2010			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
	11/15/2010	INC000000122162	N/A	N/A	N/A		

Incident Summary

On 11/15/10, at approximately 1:00 am in the morning, an Environmental Management Services employee stated that he noticed that there were two desktop computers missing from their normal location in the Decontamination Room. The two computers were described as black and gray in color, and both were fully functional with monitors, hard drives, key pads and mice.

The employee was unable to give any additional information and does not know if the computers were relocated, or the exact time when he last saw them. The employee was advised to contact his supervisor to see if the computers were relocated. If not, the supervisor will be required to submit a Report of Survey, which will be followed by a police investigation, to determine if criminal activity has occurred. Also, it is unknown at this time if the computers contained any patient information.

Incident Update

12/10/10:
The computers were not relocated but stolen from the Decontamination Room in the Supply, Processing and Distribution Section (SPD). The monitors and keyboards were also taken. The VA Police interviewed the users and confirmed that no patient information was stored on the computers. All of the information stored on the computer hard drives was related to SPD.

The computers were last used during the week prior to when they were discovered missing and were apparently stolen during the weekend. At the time the computers were taken, there were no recording devices available in the area. Since the incident, recording cameras have been installed and the locks have been changed. A Report of Survey has been filed. The VA Police investigated and filed a report.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000054916	Privacy	VISN 08 Tampa, FL	11/21/2010			High

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	55	0

Incident Summary

On 11/21/10, the Acting Surgery Service Chief reported to the weekend Administrative Officer that a digital camera used by the service could not be located. It contained 69 Veterans' PII and PHI. The Veterans had given permission for the photographs.

Incident Update

12/01/10:
The camera is still missing. The PO met with staff and viewed images on a second camera used by the Surgery Service. Based on the images on the second camera, they were able to remove 17 patients from the list of Veterans affected by this loss. As of 11/30/10, there are 52 patients' images, full names, full SSNs and DOBs believed to be on this lost camera. Fifty-two (52) Veterans will receive a letter offering credit protection services.

12/02/10:
The final count revealed a total of 55 Veterans so 55 Veterans will receive a letter offering credit protection services.

12/13/10:
The Plastic Surgery Clinic is held one afternoon a week and patients have before and after photographs taken. Normally the data is downloaded off the camera into CPRS within 24 hours after the close of the clinic, however the employee responsible for downloading the data recently accepted another position and no one else knew how to download the data. It was last downloaded approximately three weeks earlier. Staff has been educated on the process for downloading the photographs from the camera and clearing the camera of all images. A standard operating procedure (SOP) is currently under draft for the proper use and protection of the information and equipment. The data from the camera will now be downloaded immediately following the procedure.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000054928	Missing/Stolen Material (Non-Equipment)	VISN 16 Little Rock, AR	11/22/2010	11/29/2010		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
	11/22/2010	INC000000123270	N/A	N/A	N/A		

Incident Summary

A VA employee discovered an unencrypted laptop missing on 11/22/10. The laptop had been stored in a corridor of the Radiology Department. The laptop was only used to connect to CPRS/VISTA to enter electronic iMED consents for procedures. The cable lock was broken and it was reported last seen on 11/19/10 so it appears to have been stolen over the weekend. It was reported that the system was not used to store VA sensitive or PHI data.

Incident Update

11/22/10:
The laptop did not contain PII/PHI information. The system is primarily used by two Advanced Practice Nurses who assist patients reporting for procedures with electronic consent via iMED. IMed Consent is a function within Computerized Patient Record System (CPRS)/Vista Imaging so when the consent is scanned it is automatically stored within CPRS and not stored on the device.

Resolution

The VA Police have performed an initial assessment of area. To date, there are no leads. It is believed no VA sensitive data is at risk.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Score	Risk Category
SPE000000055005	Mishandled/ Misused Electronic Information	VISN 12 Chicago, IL	11/23/2010			High

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
	11/23/2010	INC000000123482	N/A	N/A	N/A	0	878

Incident Summary

Employees of Orthopedics Department maintain a calendar of patients on Yahoo.com Patient identifiers are used and it is not known how many patients are affected.

Incident Update

11/23/10:
On11/23/10, it was reported that Chicago HCS employees in the Orthopedics Department maintained a calendar of patients' data on Yahoo.com. The information stored includes full names, dates of surgery, types of surgery and last 4 of SSN for over 1000 patients. This information is stored on Yahoo.com and has been stored on the site since July 2007. Preliminary investigation reveals that four residents were sharing the same user account and password to access the data. A meeting was set up between the ISO, Chief of Surgery and Chief Orthopedics Resident. The Chief Orthopedics Resident was able to logon to Yahoo and the ISO was able to view the calendar. The Chief Orthopedics Resident notified the other residents involved that entering information into the calendar was to immediately cease. The Chief Orthopedics Resident is in the process of printing every calendar entry and will provide them to the ISO. Once completed, all entries in the Yahoo calendar will be deleted. The password word to the account has been changed. The ISO explained to the Chief of Orthopedics Resident that a shared folder was available on the secure VA network to store patient information and an Excel calendar was setup for scheduling.

11/24/10:
The VA NSOC blocked access to this external website at 7:45 a.m.

11/29/10:
The information was deleted from the web page. The PO is waiting on the final count in order to provide notification to the patients. The preliminary count is 1,730 patients.

12/02/10:
After review and removal of duplicate names, the number of unique patients' information that was on the Yahoo calendar was 878. The password to the Yahoo calendar was not changed during the three (3) years of use by rotating residents. The 878 patients will receive a letter of notification.

Total number of lost Blackberry incidents	19
Total number of internal un-encrypted e-mail incidents	60
Total number of Mis-Handling Incidents	64
Total number of Mis-Mailed Incidents	78
Total number of Mis-Mailed CMOP Incidents	5
Total number of IT Equipment Inventory Incidents	4
Total number of Missing/Stolen PC Incidents	4
Total number of Missing/Stolen Laptop Incidents	7 (6 encrypted)