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

April 30 - June 3, 2012

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000074817	Mishandled/ Misused Physical or Verbal Information	VISN 08 Bay Pines, FL	4/30/2012	5/3/2012	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
VANSOC0565872	4/30/2012	INC000000211080	N/A	N/A	N/A		1

Incident Summary

Veteran A received a copy of Veteran B's appointment reminder letter along with his own. The letter contains Veteran B's full name, mailing address, last four digits of the SSN and information related to his appointment (clinic location, date and time). Veteran A will return to facility tomorrow with the mis-mailed letter.

Incident Update

04/30/12:
Veteran B will be sent a notification letter.

NOTE: There were a total of 133 Mis-Mailed incidents this reporting period. Because of repetition, the other 132 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 information was returned to the Privacy Officer. The employees who are responsible for mailing out these type of letters have been asked to apply additional safeguards when mailing out Veteran's personal information. The supervisors were instructed to discuss this incident with all staff. A HIPAA notification letter was mailed to Veteran B.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000074830	Mishandled/ Misused Physical or Verbal Information	VISN 08 West Palm Beach, FL	4/30/2012	5/8/2012	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
VANSOC0565974	4/30/2012	INC000000211114	N/A	N/A	N/A	1	

Incident Summary

A VA employee handed a Benefit Travel Worksheet to Veteran A that contained the full SSN of Veteran B.

Incident Update

04/30/12:
Veteran B will be sent a letter offering credit protection services.

NOTE: There were a total of 168 Mis-Handling incidents this reporting period. Because of repetition, the other 167 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 copy of the worksheet was provided to the Privacy Officer (PO). It was determined that this was a result of human error. Veteran A verified with the Medical Administration Service (MAS) Supervisor that all of the other information on the form belonged to him and was correct, except for the SSN. The PO advised the appropriate staff to review and verify that the information on the form is correct before it is handed over to the Veteran. A letter offering credit monitoring services was mailed to the Veteran on 05/07/12.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000074842	Mishandled/ Misused Physical or Verbal Information	VISN 16 Fayetteville, AR	4/30/2012	5/29/2012	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
VANSOC0566007	4/30/2012	INC000000211164	N/A	N/A	N/A		290

Incident Summary

Envelopes that had Veterans' address labels on them were mailed out with different Veterans' names and addresses on the letters inside. All letters seem to come from the Fort Smith Community Based Outpatient Clinic (CBOC) but were addressed to Veterans at the Mount Vernon CBOC. The Privacy Officer (PO) has not determined exactly how many Veterans are involved.

Incident Update

05/07/12:
This may involve 500 Veterans. The data that was involved is full name, appointment time, appointment clinic, home address, and last four digits of the SSN. An exact count is being made. The mailroom was doing a mass mailing of Women Veterans Day flyers and accidently mailed out appointment letters in the pre-labeled envelopes addressed to the women Veterans.

05/08/12:
The Privacy Officer reports the new estimate to be between 350 and 400 individuals involved. The final count is expected by 05/10/12.

05/10/12:
There were a total of 362 appointment letters that went out to the wrong addresses. Of those, 72 were returned unopened. The appointment did not include either full SSNs or dates of birth. The 290 Veterans will be sent letters of notification.

Resolution

The PO re-educated the mail room staff on the importance of ensuring that the correct letter is placed in the correct envelope. The HIPAA notification letters were mailed on 05/29/12.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000074880	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Tucson, AZ	5/1/2012	5/18/2012	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
VANSOC0566196	5/1/2012	INC000000211314	N/A	N/A	N/A		1

Incident Summary

Patient A received a Medline Industries medical supply package 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. Tucson Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a Medline packing error.

Incident Update

05/01/12:
Patient B will be sent a notification letter due to PHI being exposed.

NOTE: There were a total of 8 Mis-Mailed CMOP incidents out of 7,683,769 total packages (11,354,422 total prescriptions) mailed out for this reporting period. Because of repetition, the other 7 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
SPE000000074984	Missing/Stolen Equipment	VISN 06 Durham, NC	5/2/2012	5/11/2012	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
VANSOC0566639	5/2/2012	INC000000211688	N/A	N/A	N/A		

Incident Summary

In April of 2011, a pallet of Tangent all-in-one devices, which includes a CPU, was delivered to the Durham VA warehouse, at which point VA warehouse staff signed as having received the pallet. On 05/10/11, OIT staff went to collect the equipment from the warehouse and discovered that one of the all-in-one devices was missing. It is unclear whether the device was missing before it was received or went missing after it was received by the VA. We are certain that the device was never connected to the VA network and did not contain any kind of VA information, sensitive or otherwise. These devices were part of a purchase order for multiple VISN 6 facilities so there is the possibility that it was delivered to another VA site. Durham warehouse staff are contacting the other VISN 6 sites to determine if that is the case.

The Facility Chief Information Officer (CIO) contacted VA Police and Acquisition services in an attempt to track down the all-in-one device. The VA Police service is currently investigating this incident. OIT service is completing a Report of Survey (ROS) on the missing device.

Incident Update

05/02/12:
There is no VA data on the device. VA Police and Acquisitions are investigating.

Resolution

The Report of Survey is in progress. It was determined that the other sites under the purchase order did not receive the computer either. No information is at risk. The device in question never contained any VA information and was never connected to any VA network.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000075469	Missing/Stolen Equipment	VISN 18 Phoenix, AZ	5/14/2012	5/14/2012	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
VANSOC0569054	5/14/2012	INC000000213861	N/A	N/A	N/A		

Incident Summary

An incident occurred sometime between 04/19/12 through 04/26/12. The incident was reported to the Information Security Officer (ISO) on 05/14/12 at approximately 8:20 AM. The ISO office was informed that a PC tower was discovered missing. The PC was located in the hospital's Emerald Clinic conference room. Dieticians noticed the tower was missing on 04/26/12, however, a Dietician remembers using the tower on 04/19/12. A Report of Survey was completed and the ISO has requested a copy of that document for further details and help direct interviews. The Chief Information Officer (CIO) for local OIT has informed the ISO that his team has attempted to connect to the tower without any response. According to the Network Administrator, the last time the PC was seen on the network was five months ago. Hospital towers are not encrypted and if the user had saved (directly) to the desktop, those items are not saved on the server. However, local policy expectation is that all work should be saved directly to the server. The ISO is gathering more details as they are presented to the ISO office. The ISO is highly recommending that conference room towers are cable locked, moving forward.

Resolution

The clinic has been advised to ensure that the door is locked at all times. They are asking local OIT for tower locks to secure the towers. The ISO will inform the service to remind employees of the importance of immediately reporting potentially missing equipment to the local OIT Supervisor and the ISO office.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000075627	Missing/Stolen Equipment	VISN 20 Spokane, WA	5/17/2012	5/17/2012	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
VANSOC0569659	5/17/2012	INC000000214636	N/A	N/A	N/A		

Incident Summary

The facility Chief Information Officer (CIO) reported that the VA Chief of Police was contacted by an employee who stated that he saw someone leaving one of the facility's leased buildings with computer equipment, indicating a potential property theft. The Chief of Police informed the Acting Medical Center Director, who then initiated an immediate investigation. The primary concern is whether the computer equipment contains Personally Identifiable Information (PII) or Protected Health Information (PHI). The CIO's preliminary investigation indicates that the stolen computer was brand new and did not contain any PII/PHI. The Office of Inspector General is at the building taking statements from staff and confirming the CIO's findings. The investigation will be completed the morning of 05/18/12. It was later confirmed by the person reporting the incident that there was no data loss.

Incident Update

05/17/12:
The PC was brand new and did not contain any VA information.

Resolution

No security breach occurred.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000075843	Mishandled/ Misused Physical or Verbal Information	VISN 18 Albuquerque, NM	5/22/2012		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
VANSOC0570213	5/22/2012	INC000000215460	N/A	N/A	N/A		290

Incident Summary

A VA employee did not secure/safeguard a cardex at the end of the work day on 05/17/12. When the employee came to work on 05/18/12, the cardex could not be located. This cardex contained names, last four digits of the SSN, primary diagnosis and provider name. It is reported that list could possibly contain 290 names.

Incident Update

05/25/12:
The search for the hard copy of the cardex continues. This was reported to the VA Police and it is currently being investigated. There is a possibility that a break-in occurred. The Privacy Officer (PO) has an electronic copy and can recreate the list for notifications.

05/30/12:
Two-hundred and ninety patients will receive letters of notification due to protected health information (PHI) being potentially compromised.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000075961	Missing/Stolen Equipment	VISN 08 Gainesville, FL	5/24/2012	6/7/2012	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
VANSOC0570585	5/24/2012	INC000000215941	N/A	N/A	N/A		

Incident Summary

During a routine inventory one laptop and five Palm Pilots were noticed missing from the Research Service. The laptop was bought in 2004 and was probably not encrypted. The Information Security Officer (ISO) is waiting on confirmation from the Research Service for more information.

Incident Update

05/24/12:
The laptop was purchased in 2004 and believed to be not encrypted due to its age. A Report of Survey has been filed. This is believed to be an inventory documentation error, however the ISO is investigating.

05/07/12:
The laptop and palm pilots were not encrypted. According to the Research Service, they did not contain VA sensitive information.

NOTE: There were a total of 3 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 2 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Resolution

The ISO is working with Research on ensuring the importance of device control.

Total number of Internal Un-encrypted E-mail Incidents	125
Total number of Mis-Handling Incidents	168
Total number of Mis-Mailed Incidents	133
Total number of Mis-Mailed CMOP Incidents	8
Total number of IT Equipment Inventory Incidents	3
Total number of Missing/Stolen PC Incidents	4
Total number of Missing/Stolen Laptop Incidents	8 (8 encrypted)
Total number of Lost BlackBerry Incidents	34
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	0