DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Incident Resolution Service

Monthly Report to Congress of Data Incidents

June 2 - 29, 2014

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000104802	Mishandled/ Misused Physical or Verbal Information	VBA St Petersburg, FL	6/2/2014	6/9/2014	

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number/Category	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0606560	6/2/2014	INC000000373066 Category 6 -	N/A	N/A	N/A	1	

Incident Summary

The Regional Office (RO) sent a Veterans Claims Assistance Act of 2000 (VCAA) letter to Veteran A, which had attached another VCAA letter for Veteran B. Veteran B's name and full SSN were compromised.

Incident Update

06/02/14:
The Incident Resolution Service Team determined that Veteran B will be sent a letter offering credit protection services.

Resolution

The Team Coach spoke with the responsible employee, including the Mail Room personnel on the importance of double-checking all documents that leave the RO building. The coaches will continue to work on this issue will all personnel.

DBCT **DBCT Decision Date:** N/A

No DBCT decision is required. This is informational for Mis-Mailed incidents and is the representative ticket. There were a total of 143 Mis-Mailed incidents this reporting period. Because of repetition, the other 142 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.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000104831	Mishandled/ Misused Physical or Verbal Information	VISN 06 Durham, NC	6/2/2014	7/2/2014	

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number/Category	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0606588	6/2/2014	INC000000373342 Category 6 -	N/A	N/A	N/A	1	

Incident Summary

Veteran A and Veteran B were seen in the same clinic on the same day. Veteran A received a printed prescription intended for Veteran B containing full name, full SSN, and date of birth.

Incident Update

06/02/14:
The Incident Resolution Service Team determined that Veteran B will be sent a letter offering credit protection services.

Resolution

The matter was referred to the Service Chief for action. The team plans to provide education and a reminder to all employees in the section.

DBCT **DBCT Decision Date:** N/A

No DBCT decision is required. This is informational for Mis-Handling incidents and is the representative ticket. There were a total of 101 Mis-Handling incidents this reporting period. Because of repetition, the other 100 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.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000104837	Mishandled/ Misused Physical or Verbal Information	VISN 10 Chillicothe, OH	6/2/2014	7/2/2014	

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number/Category	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0606592	6/2/2014	INC000000373264 Category 6 -	N/A	N/A	N/A		1

Incident Summary

The Consolidated Mail Outpatient Pharmacy (CMOP) mailed one bottle of medication intended for Veteran A to Veteran B. Veteran B contacted VA and the medication was returned to the Medical Center. A new medication was sent to Veteran A.

Incident Update

06/02/14:
The Incident Resolution Service Team has determined that Veteran A will be sent a HIPAA notification letter since his name and medication information was disclosed.

Resolution

Pharmacy staff contacted the Veterans involved to explain the incident and to make sure that medications were taken appropriately.

DBCT **DBCT Decision Date:** N/A

No DBCT decision is required. This is informational for Mis-Mailed CMOP incidents and is the representative ticket. There were a total of 5 Mis-Mailed CMOP incidents out of 6,464,834 total packages (9,545,209 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	Date of Initial DBCT Review
PSETS0000104905	Mishandled/ Misused Physical or Verbal Information	VISN 17 San Antonio, TX	6/3/2014	6/3/2014	

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number/Category	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0606655	6/3/2014	INC000000373704 Category 4- Improper	N/A	N/A	N/A		161

Incident Summary

During an on-camera interview on the evening of 06/02/14 with 4 VHA employees (identities disguised), the News 4 Reporter from WOAI stated "last week a source with ties inside the San Antonio VA gave News 4 a partial recall delinquency list. It shows 150 Veterans needing medical care in the beginning of May". The Reporter went on to say, "We spoke with Veterans on this delinquency list." The facility is in the process of attempting to obtain the list of patients the Reporter obtained "illegally" and to determine the source. Further information will be added as soon as it is available.

Incident Update

06/09/14:
This is still being investigated by the Privacy Office. The Privacy Officer (PO) has been in contact with the Reporter and is attempting to retrieve the information. As of 06/06/14, the Reporter has not provided the information requested. The PO is requesting, at the very least, to have the names of the individuals whose information was disclosed without authorization so that VA can begin the notification process.

06/10/14:
The Incident Resolution Service Team determined that, based on the VA Breach Criteria, this would be a breach and require notification, since the full name and partial SSN were disclosed. The 161 Veteran will receive a HIPAA letter of notification. The Data Breach Core Team (DBCT) concurred.

DBCT **DBCT Decision Date:**

06/10/14:
No DBCT decision needed. This is informational due to the number of Veterans affected.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000105163	Missing/Stolen Equipment	VISN 20 Seattle, WA	6/10/2014	6/23/2014	

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number/Category	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0606911	6/10/2014	INC000000375392 Category 6 -	N/A	N/A	N/A		

Incident Summary

A Report of Survey (ROS) was signed on 05/23/14 and provided to the Information Security Officer (ISO) on 06/03/14. After checking the 55 items, two appear data capable. One item was previously reported when it was found missing on PSETS0000100736 in February 2014. The other item which is being reported on this NSOC ticket is a Ricoh printer/copier/facsimile which contains a hard drive and thus may contain sensitive information. The ISO has not yet confirmed where this fax machine was used or for what purpose. Leadership has been notified and the Service Line and the IT Department have been asked to work together to find out what happened, as usually all Ricoh devices fall on the IT Department's inventory, but this was still on the Service Line's inventory.

Incident Update

06/16/14:
The ISO is still investigating the incident.

Logistics responded that the device should not have a hard drive, per the vendor. However, internet research and a copy of the equipment model's manual contradicted that vendor statement. Per the manual, there is a hard drive. The ISO requested ITOS to check other similar models deployed at the facility to confirm or deny that the equipment had a hard drive.

Resolution

No violation was found. The device has RAM but no ability to write to memory. There was no data at risk.

DBCT **DBCT Decision Date:** N/A

No DBCT decision needed. This stays on as informational for missing equipment.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000105386	Missing/Stolen Equipment	VISN 19 Denver, CO	6/16/2014		6/24/2014

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number/Category	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0607125	6/16/2014	INC000000376774 Category 1 -	N/A	N/A	N/A		

Incident Summary

During a recent inventory, OIT and Biomed Engineer discovered missing equipment. The missing laptop is part of an Audiology package: HP ProBook Laptop, Bridge Ear, and Printer. The whole package was still in its original packaging minus the laptop, stored in a Community Based Outpatient Clinic last inventoried on 11/02/12. The laptop software was the original manufacturer's software, Natus Medical and not VA imaged. The laptop was not encrypted; OIT and Biomed Engineer believed that the equipment has never been used and no VA patients' data stored on the hard drive. The Information Security Officers (ISO) and Privacy Officer (PO) will update this ticket as soon as we have more information regarding this missing equipment.

Incident Update

06/16/14:
The Incident Resolution Service Team determined that, at the present time, it does not appear that a data breach occurred. The search for laptop continues.

06/24/14:
The laptop was stolen and was discovered missing during inventory. There was no VA data on laptop.

DBCT **DBCT Decision Date:** N/A

No DBCT decision needed. This stays on as informational for missing equipment.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000105501	Missing/Stolen Equipment	VISN 23 Iowa City, IA	6/18/2014		6/24/2014

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number/Category	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0607232	6/18/2014	INC000000377494 Category 1 -	N/A	N/A	N/A		

Incident Summary

During a routine inventory of VA Police equipment, it was found that two (2) devices capable of storing VA data could not be located. Both were digital pocket cameras. A Report of Survey (ROS) has been started for the devices. Logistics and the VA Police were contacted as part of the ROS team.

Incident Update

06/23/14:
There is no indication the devices were ever used for anything other than training, so it is very unlikely that anything was stored on the cameras. VA Police stated the devices were capable of being encrypted, however, it is unknown if encryption was applied. As soon as the Information Security Officer (ISO) can locate the type and brand name, the ISO can confirm the type of encryption or the encryption level.

On 05/08/13, the items were in the VA Police Deputy Chief's Office. According to the inventory list, they were last inventoried 08/24/13. They were currently being inventoried for the incoming Acting Chief of Police and Accountability Official.

Twenty devices were bought. There are 15 FTE in that service and were to be assigned to a VA Police Officer by serial number which was located in their training records. It is unknown if they were issued to each officer. Eighteen are accounted for and still have their original box and two have not been accounted for. Per the interview with the VA Police Accountability Officer, one was used for a demonstration when they were bought in 2012 and returned to the Deputy Chief's Office and one may have been removed by an officer and not returned for inventory.

DBCT **DBCT Decision Date:** N/A

No DBCT decision needed. This stays on as informational for missing equipment.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000105506	Missing/Stolen Equipment	Employee Education Services/ EES St. Louis, MO	6/18/2014	6/20/2014	

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number/Category	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0607237	6/18/2014	INC000000377509 Category 6 -	N/A	N/A	N/A		

Incident Summary

During FY14 Equipment Inventory Listing (EIL) Inventory the following items were not located: Server; Cisco Content Engines, Cisco Routers. The equipment was last located on 05/21/13 as part of EIL Inventory.

Incident Update

06/19/14:
The Information Security Officer (ISO) was sent a follow-up email stating the item missing was a server rack, not a server. The ISO checked to see if the content engines or routers contain personally identifiable information (PII). The ISO received email confirmation that no PII is stored on the missing equipment. The stored content would have been training videos with no PII.

Some of the Cisco routers have been located so that is down to one missing.

The Incident Resolution Service Team determined that no data breach occurred since there was no PII on the devices.

Resolution

The missing equipment did not contain PII.

DBCT **DBCT Decision Date:** N/A

No DBCT decision is required. This is informational for IT Equipment Inventory incidents and is the representative ticket. There were a total of 2 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 1is not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Total number of Internal Un-encrypted E-mail Incidents	93
Total number of Mis-Handling Incidents	101
Total number of Mis-Mailed Incidents	143
Total number of Mis-Mailed CMOP Incidents	5
Total number of IT Equipment Inventory Incidents	2
Total number of Missing/Stolen PC Incidents	2 (2 encrypted)
Total number of Missing/Stolen Laptop Incidents	4 (4 encrypted)
Total number of Lost BlackBerry Incidents	23
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	