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

Monthly Report to Congress of Data Incidents

March 3 - 30, 2014

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000101142	Mishandled/ Misused Electronic Information	VISN 04 Altoona, PA	3/3/2014	3/7/2014	

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
VANSOC0603077	3/3/2014	INC000000350358 Category 6 -	N/A	N/A	N/A	1	

Incident Summary

Veteran A reported he found Veteran B's medical report on a CD from Release of Information (ROI) that contained his military records. The information was scanned from his VA medical record. The information at risk included Veteran B's name, date of birth, partial SSN and protected health information (PHI).

Incident Update

03/03/14:
Due to medical information and date of birth being exposed, the Incident Resolution Team has determined that Veteran B will be sent a letter offering credit protection services.

Resolution

The one document belonging to Veteran B was removed from Veteran A's record and scanned into the Veteran B's record immediately upon notification of this error. All staff involved in the ROI and Scanning/Indexing process were informed of the error and fact finding was initiated. Veteran A did return the disc back to ROI same day as the Chief of Health Information Management (HIM) became aware of the breach. Appropriate staff did immediately apologize to Veteran A, both in person and on the phone.

HIM ROI and Scanning /Indexing staff have been re-educated regarding basic office procedures of making a copy to work from and returning the Veteran's copy of his military record back to the Veteran immediately. All involved staff have been reminded to check for patient identification on all documents prior to scanning/indexing. Staff involved who have provided service to Veteran A since the breach was brought to our attention have apologized to Veteran A.

In conclusion, we cannot conclusively say how the one document on Veteran B was misfiled with Veteran A's 325 pages of documents. We have reminded all staff to follow all procedures and make every effort that this not happen again. All staff verbalized understanding of the expectations set. The letter to Veteran B offering credit monitoring was sent on 03/07/2014.

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 99 Mis-Handling incidents this reporting period. Because of repetition, the other 98 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
PSETS0000101150	Mishandled/ Misused Physical or Verbal Information	VBA St Louis, MO	3/3/2014	3/6/2014	

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
VANSOC0603085	3/3/2014	INC000000350374 Category 6 -	N/A	N/A	N/A	1	

Incident Summary

Veteran A received Veteran B's mail. The Information at risk included Veteran B's name, full SSN and protected health information (PHI).

Incident Update

03/03/14:
The Incident Resolution Team has determined that Veteran B will be sent a letter offering credit protection services.

Resolution

The Privacy Officer (PO) is unable to determine which employee sent the letter, however the facility has taken measures to prevent this from happening again, including re-education and retrieval.

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 111 Mis-Mailed incidents this reporting period. Because of repetition, the other 110 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
PSETS0000101278	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Hines, IL	3/6/2014	3/14/2014	

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
VANSOC0603202	3/6/2014	INC000000351545 Category 4- Improper	N/A	N/A	N/A		1

Incident Summary

Patient A received prescription paperwork intended for Patient B. Patient B's name, address, and type of medication were compromised. Patient A reported the incident to the medical center and will return Patient B's paperwork to the medical center. Great Lakes 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

03/06/14:
The Incident Resolution Team has determined that Patient B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

The CMOP employee was counseled and retrained in proper packing procedures.

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 2 Mis-Mailed CMOP incidents out of 6,477,163 total packages (9,453,872 total prescriptions) mailed out for this reporting period. Because of repetition, the other 1 is 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
PSETS0000101351	Missing/Stolen Equipment	VISN 23 Iowa City, IA	3/7/2014		

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
VANSOC0603271	3/7/2014	INC000000351952 Category 1 -	N/A	N/A	N/A		

Incident Summary

During a routine inventory of VA Research IT equipment it was found that one (1) device (Personal Computer) capable of storing VA Data could not be located. There was no personally identifiable information (PII) or protected health information (PHI) stored on the computer. The hard drive was not encrypted. The studies conducted using the device strictly involved non-human subject research. A Report of Survey (ROS) will be conducted which includes a VA Police investigation

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 4 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 3 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000101703	Missing/Stolen Equipment	VISN 12 Madison, WI	3/19/2014	3/26/2014	3/25/2014

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
VANSOC0603606	3/19/2014	INC000000354564 Category 1 -	N/A	N/A	N/A		

Incident Summary

An equipment list audit shows a notebook computer that was purchased in 2011 for a Research project is not in the expected location. Investigation is continuing to determine what the specific project was, where the notebook currently is, whether protected health information (PHI) was being collected, and where it was stored if it was collected. There is no reason at this point to assume the computer is no longer with the VA; however, the possibility has been raised that the primary investigator may have inadvertently taken it with him when he left the VA.

Incident Update

03/20/14:
Both the staff member using the GFE laptop and the issuer of the grant (Director of the VA National Center for PTSD- Pacific Islands Division) indicate there was no PHI stored on the laptop. Per the psychologist who had been using it, the laptop was left at the facility when he terminated employment. It was never connected to the VA network. Staff connected using the Citrix gateway. The laptop was last seen in October 2013. The fact that the laptop is missing was reported to the VA Police.

Resolution

Investigation is still continuing; however, while the laptop does not appear to have been encrypted, it did not contain PHI and did not connect to the VA network. Policies and processes are being put in place to ensure tracking of non-IRMS equipment and confirmation of proper transfer of VA records/documentation when an employee leaves the VA.

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

03/25/14:
The laptop contained no sensitive data. This is not a data breach. 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
PSETS0000101775	Missing/Stolen Equipment	VISN 22 Long Beach, CA	3/20/2014	3/24/2014	3/25/2014

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
VANSOC0603667	3/20/2014	INC000000357163 Category 4- Improper	N/A	N/A	N/A		

Incident Summary

After exhaustive search including Information Security Officer (ISO) information verification with Biomed, Varian vendor and IT customer solutions, Radiology Therapy Technician conducting the inventory, concluded that the 2 computers used to work in conjunction with Varian medical equipment were missing. During interview with Varian representative, the ISO determined that the missing computers were storing personally identifiable information (PII) or protected health information (PHI) only temporarily as all the data was routinely backed up into their server by design. The computers had been replaced and were stored in a side room for further disposal.

Incident Update

03/20/14:
The PCs do not store patient information. No breach has occurred.

Resolution

No data breach occurred.

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

03/25/14:
There was no information on the two PCs. 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
PSETS0000101954	Unauthorized Physical or Verbal Access	VISN 01 West Haven, CT	3/26/2014		4/1/2014

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
VANSOC0603826	3/26/2014	INC000000356377 Category 1 -	N/A	N/A	N/A		

Incident Summary

A nurse lost the InteliKey to the G-4-E medication room.

Incident Update

03/27/14:
There are narcotics under double lock within the room. Non-narcotic medications are not locked within the room. The lock has not been reconfigured at this time. There are no cameras in the area. There may have been standard protected health information (PHI) like name and medication name that you would find on patient medications.

They will disable the key and audit the door this morning to see if the key has been used since it went missing.

03/31/14:
The lost key was used to access the medication room over the weekend. VA Police are investigating.

04/04/14:
The PO is awaiting the results of the VA Police investigation.

04/08/14:
The nurse received her replacement key the morning of 3/31/14. Her old key was used one time in the G4E Medroom on 3/30/14. This is her area and was during her assigned tour. She was interviewed and said she did not have it at the time. This leads us to believe another staff person might have picked it up accidently. At this time the key in deactivated and will not work.

The Controlled Substance Inspection Coordinator conducted a full inventory of the Medroom and the Pyxis activity for the unit as well as the nurse involved was reviewed. No suspicious activity or evidence of diversion was found. All drugs were accounted for.

The PO has asked the Nurse Manager of the unit to conduct a key inventory with the Lock Shop to ensure all keys are accounted for. He is waiting on an update from her when it is done. At this time she has accounted for 31 out of 38 keys. She expects to finish her counts today or tomorrow, except for two nurses who are out on Annual Leave.

Resolution

The lost key was deactivated and a new key was issued.

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

04/01/14:
Presented to the DBCT. Keep on report as investigation continues since PHI was in the medication room.

04/08/14:
The DBCT determined that there was a low risk of compromise since the employees all had access to PHI and could obtain it much easier than taking it from the medication room.

Total number of Internal Un-encrypted E-mail Incidents	87
Total number of Mis-Handling Incidents	99
Total number of Mis-Mailed Incidents	111
Total number of Mis-Mailed CMOP Incidents	2
Total number of IT Equipment Inventory Incidents	4
Total number of Missing/Stolen PC Incidents	0
Total number of Missing/Stolen Laptop Incidents	0
Total number of Lost BlackBerry Incidents	17
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	0