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

November 4 - December 1, 2013

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000096536	Mishandled/ Misused Physical or Verbal Information	VISN 01 Bedford, MA	11/4/2013	11/18/2013	

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
VANSOC0598713	11/4/2013	INC000000324141	N/A	N/A	N/A	1	

Incident Summary

A Private company employee called to report that a prescription intended for CVS was sent to her company's fax machine. Fax did not have coverage. Fax number was off by 1 number. The Privacy Officer (PO) sent employee a postage paid return envelope to return fax. PO followed-up with provider reminding her to double check fax numbers and always use HIPAA compliant fax coverage. Fax coverage sent to provider.

Incident Update

11/04/13:
Due to medical information and date of birth being exposed, Veteran A will be sent a letter offering credit protection services.

Resolution

PO followed-up with provider reminding her to double check fax numbers and always use HIPAA compliant fax cover page. Fax cover page sent to provider. PO did in-service training reminding staff on appropriate safeguards for faxing.

DBCT

No DBCT decision needed. This is a representative ticket. There were a total of 118 Mis-Handled incidents this reporting period. Because of repetition, the other 117 are not included in this report, but are included in the "Mis-Handled 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
PSETS0000096571	Missing/Stolen Equipment	VISN 20 Seattle, WA	11/4/2013		11/12/2013

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
VANSOC0598749	11/4/2013	INC000000324324	N/A	N/A	N/A		

Incident Summary

A Report of Survey (ROS) was turned in and passed to the Information Security Officer (ISO) for review. Although several computers and hard drives are listed, most are from 2002 to 2006 and thus present little to no risk of data loss at this late date. The newest item on the list is a laptop from 2010 checked out to a clinician. This VA laptop is encrypted, however, it is unclear if anyone reached the clinician to see if the laptop is still in his possession or what types of data were in use on it.

Incident Update

11/05/13:
The ROS contains 19 laptops; six of the laptops were never assigned to staff or used. The others appear to have been turned in previously. There is one laptop from 2010 checked out to a clinician. This laptop is encrypted. The clinician has not been contacted at this time to see if the laptop is still in his possession and/or what types of data were on it.

11/06/13:
The one laptop listed as missing on the first ROS has been found. After the ISO provided the Research and Development (R&D) Department with a listing of equipment, they contacted and confirmed that the laptop is in the possession of the VA staff member it is checked out to and the encryption is current. This laptop has been found. One of the workstations listed in the first report is also still in the possession of the individual it was loaned to and thus is also no longer missing. The ISO anticipates more equipment will be located in the possession of the VA staff it is checked out / loaned out to.

11/08/13:
Two more pieces of equipment (non-laptops) have been located by the R&D Department.

11/15/13:
R&D Staff have confirmed one more laptop is in the possession of the individual listed as having it checked out. IT has assigned administrative staff to work on the inventory.

DBCT

No DBCT decision needed. This is a representative ticket. There were a total of 6 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 5 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
PSETS0000096603	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Hines, IL	11/5/2013	11/19/2013	

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
VANSOC0598784	11/5/2013	INC000000324453,	N/A	N/A	N/A		1

Incident Summary

Patient A received a prescription intended for Patient B. Patient B's name and type of medication was compromised. Patient A reported the incident to the medical center and a replacement has been requested for Patient B. 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

11/05/13:
Veteran B will be sent a notification letter.

Resolution

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

DBCT

No DBCT decision needed. This is a representative ticket. There were a total of 8 Mis-Mailed CMOP incidents out of 5,820,835 total packages (8,825,750 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.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000096717	Missing/Stolen Equipment	VACO Field Program Office Denver, CO	11/7/2013	11/18/2013	11/12/2013

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
VANSOC0598892	11/7/2013	INC000000325152	N/A	N/A	N/A		

Incident Summary

A laptop with Veteran information was stolen out of a vendor's car. It was reported yesterday that on or about 09/06/13, an unencrypted laptop was stolen from a vendor who provides fee for service to the VA. It is estimated that 200 Veterans' information, including names and medical information, was stored on this laptop.

Notes:
1. The vendor is a covered entity.
2. The vendor is responsible for handling the credit monitoring.
3. This is a HITECH issue as it covers more than 500 total individuals (200 Veterans).
4. The notification to VA regarding this incident is extremely late as it should have been reported within 24 hours of the loss. Apparently the laptop was stolen on 09/06/13 but at that time it was believed that the information was encrypted. It wasn't until recently that they found out the information was not encrypted.

Incident Update

11/19/13:
The vendor sent the letters on 11/05/13. The vendor also distributed a press release to various media outlets and has a posting of the incident on their website.

Resolution

The Contracting Officer (CO) contacted the Privacy Officer (PO) and Information Security Officer (ISO) as soon as the violation was reported by the contractor. The Contracting Officer (COR) and ISO working together on lessons learned and any follow-up actions.

DBCT

This is informational as it was not a VA data breach. It was a vendor's data breach. The DBCT requested and received copies of the actual letter that the vendor sent, the press release and the date that HHS/OCR was notified.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000096892	Mishandled/ Misused Physical or Verbal Information	VISN 04 Philadelphia, PA	11/13/2013		11/19/2013

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
VANSOC0599059	11/13/2013	INC000000326223	N/A	N/A	N/A		

Incident Summary

The Privacy Officer (PO) received a phone call from the Federal Correctional Complex in Petersburg, VA regarding a photocopy of a Personal Identity Verification (PIV) card belonging to a Philadelphia VA employee. The Federal Correctional Complex staff intercepted the inmate's outgoing mail and the photocopy of the PIV card was inside the envelope. The Special Investigative Lieutenant "GOOGLED" the name on the PIV card and discovered the employee worked at the Philadelphia VA from the Facebook page.

Incident Update

11/13/13:
The employee did not report a lost card. The photocopy of the card was found in outgoing mail at the Federal Correction Complex. The Federal Correctional Complex was alerted because the return address on the letter was not address of the complex. The local VA Police are working with the Correctional Complex to determine how many times the employee had contact with the inmate.

11/18/13:
An internal investigation is being conducted by the local VA Police. The employee did not report a missing PIV card. The employee photocopied the PIV card.

12/04/13:
The PO is still waiting for the Police report.

DBCT

11/19/13 - DBCT waiting for more information from the Police report.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000097129	Mishandled/ Misused Physical or Verbal Information	VISN 09 Lexington, KY	11/20/2013	11/27/2013	

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
VANSOC0599272	11/20/2013	INC000000327656	N/A	N/A	N/A		1

Incident Summary

Veteran A received Veteran B's appointment letter. The letter contained Veteran B's full name, address, last four digits of the SSN and medical clinic name. This involved one Veteran. It was outside of VA control for more than 72 hours and was recovered.

Incident Update

11/20/13:
Veteran B will receive a HIPAA notification letter.

Resolution

The employee has been re-educated on the appropriate handling of personally identifiable information (PHI).

DBCT

No DBCT decision needed. This is a representative ticket. There were a total of 125 Mis-Mailed incidents this reporting period. Because of repetition, the other 124 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
PSETS0000097444	Mishandled/ Misused Physical or Verbal Information	VACO Field Program Office Atlanta, GA	11/26/2013		12/3/2013

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
VANSOC0599577	11/26/2013	INC000000329266	N/A	N/A	N/A		

Incident Summary

The Health Eligibility Center (HEC) has reported to our office that they discovered that a Veterans' full SSN showed through their window envelope with the address. We had them go back one month and discovered this happened to a total of 113 Veterans. The HEC reported that the facilities involved had transmitted the data with the SSN in the same block as the address. The HEC provided our office with a spreadsheet of the Veterans involved and your facility was one of these facilities.

Incident Update

12/02/13:
This ticket seems to be a "parent" ticket to several others that have been entered for the same reporting period (to date includes the following PSETS tickets: 97430, 97439, 97445, 97492, 97520)

The IRT is awaiting a call back from VHA Privacy who contacted several facilities (unknown at this time) to determine more details about this, such as is the incident the responsibility of the HEC or the individual facilities involved.

This is being left on the report for the total number of affected individuals, however the total number is the sum of the various facilities involved. Most of the "child" incidents related to this vary from 1 to 5 affected individuals.

DBCT

12/03/13:
The person in VHA privacy who contacted the facilities to put the tickets has contacted the IRT. She is having the facilities hold up on entering tickets in, as there is still some investigation going on. It seems that it is possible that the SSN may have been transmitted to the HEC in the address field. It is also possible that the letters were never even sent out by the HEC. VHA Privacy is awaiting some more information from the HEC PO.

Total number of Internal Un-encrypted E-mail Incidents	86
Total number of Mis-Handling Incidents	118
Total number of Mis-Mailed Incidents	125
Total number of Mis-Mailed CMOP Incidents	8
Total number of IT Equipment Inventory Incidents	6
Total number of Missing/Stolen PC Incidents	3
Total number of Missing/Stolen Laptop Incidents	12 (9 encrypted)
Total number of Lost BlackBerry Incidents	27
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	1