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

Monthly Report to Congress of Data Incidents

May 5 - June 1, 2014

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000103678	Mishandled/ Misused Physical or Verbal Information	VISN 01 Boston, MA	5/5/2014	5/9/2014	

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
VANSOC0605495	5/5/2014	2014-USCERTv3ZGI7X Category 6 -	N/A	N/A	N/A	1	

Incident Summary

Veteran A reported receiving Veteran B's protected health information (PHI) in an envelope along with Veteran A's PHI at Veteran A's home address. Veteran A dropped off the PHI of Veteran B to an employee. Veteran B's name, address, partial SSN and PHI were compromised.

Incident Update

05/05/14:
The Incident Resolution Service Team has determined that Veteran B will be sent a letter offering credit protection services.

Resolution

The Privacy Officer (PO) required the responsible employee to retake TMS 10136 and to receive focused Release of Information (ROI) training from the supervisor by close of business 05/09/14. The PO talked with Veteran on telephone on 05/07/14 and mailed the credit monitoring letter to the Veteran on 05/08/14.

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 159 Mis-Mailed incidents this reporting period. Because of repetition, the other 158 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
PSETS0000103687	Mishandled/ Misused Physical or Verbal Information	VISN 12 Chicago, IL	5/5/2014	5/30/2014	

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
VANSOC0605503	5/5/2014	INC000000366529 Category 6 -	N/A	N/A	N/A		1

Incident Summary

Veteran A received a copy of Veteran B's appointment schedule which contained Personally Identifiable Information (PII). The information at risk included Veteran B's name, address, partial SSN and diagnosis.

Incident Update

05/05/14:
The Incident Resolution Service Team has determined that Veteran B will be sent a HIPAA notification letter.

Resolution

The Privacy Office and Service Unit conducted Privacy re-training for the affected clerks on 05/13/14, during which they reviewed the existing facility Privacy policy and compliance guidelines. The HIPAA notification letter was forwarded to affected Veteran.

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 120 Mis-Handling incidents this reporting period. Because of repetition, the other 119 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
PSETS0000103887	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Hines, IL	5/8/2014	5/22/2014	

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
VANSOC0605694	5/8/2014	INC000000367889 Category 6 -	N/A	N/A	N/A		1

Incident Summary

Patient A received a prescription package intended for Patient B. Patient B's name, address, 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 is the result of a VAMC incorrect address transmission leading to a USPS misdelivery, not a CMOP packaging error. The medical center has been notified.

Incident Update

05/09/14:
The Incident Resolution Service Team has determined that Veteran B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

The medical center was notified to correct the mailing address on 05/08/14.

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 was a total of 1 Mis-Mailed CMOP incident out of 6,211,667 total packages 9,058,821 total prescriptions) mailed out for this reporting period. The Veteran will receive a notification letter.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000104269	Missing/Stolen Equipment	VISN 06 Asheville, NC	5/16/2014		5/20/2014

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
VANSOC0606035	5/16/2014	INC000000369752 Category 1 -	N/A	N/A	N/A		

Incident Summary

During the collection of the PCs from the Resident Quarters Buildings, it was discovered that two PCs were missing. They were last inventoried in February, 2013. The PCs were set up as unencrypted personal computers so that the Residents could connect via VPN to the medical center when they were on call after hours. It was reported that no personally identifiable information (PII)/protected health information (PHI) was stored on the computers.

Incident Update

05/19/14:
The Chief of Surgery spoke with one of the Orthopedic Residents who said he had taken one of the PCs to the Goodwill. The Police Officer went to the Goodwill store where the Resident stated that he dropped it off and found out from Goodwill that they process pallets of computers but do not keep track of serial numbers, just make and model. They have a list that shows that the same make (HP DC7100) was processed on 05/12/14. Goodwill uses Darik's Boot and Nuke (DBAN) which is a DOD-level scrubbing program to wipe the hard drive of computers they process. The system was refurbished and sold. They have no records of who purchased it.

05/20/14:
The second PC (Dell Optiplex 520 with the EE# 105400) has been located and is now in OI&T's possession.

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

05/20/14:
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
PSETS0000104385	Missing/Stolen Equipment	VISN 19 Denver, CO	5/20/2014	6/9/2014	5/27/2014

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
VANSOC0606154	5/20/2014	INC000000370462 Category 1 -	5/20/2014	Yes	Pending	239	

Incident Summary

Two biomedical device laptops were discovered missing on 05/20/14. VA Police were notified of the event. The two missing laptops were password protected but not encrypted due to being attached to biomedical devices. The laptops were located on mobile test stations in the Pulmonary Department. The portable test equipment was used when patients could not be transported to the Pulmonary Department for testing. The exact number of patients is unknown. The upper limit is 5,000 and could be as low as 350. The ticket will be updated when more information is available.

Incident Update

05/21/14:
Additional questions have been sent to the Information Security Officers (ISO) and Privacy Officer (PO) regarding the missing laptops.

Update: The laptops were not encrypted as they were attached to biomedical devices. The laptops were VA issued equipment (EE#56243 and EE#56244). The Pulmonary supervisor reported that she discovered the laptops missing on 05/20/14 but was informed by one of the technicians that she saw them missing about 2 weeks ago, exact date unknown, but thought they were being worked on. The supervisor then checked with Information Resource Management Systems (IRMS) and Bio-med to see if they had been picked up the reply was negative. The laptops were last inventoried on 04/22/14 in room 6A-144. These were standalone systems and had never been connected to the network. To the best of the facility's knowledge, the laptops were not secured with cables and it is currently unknown why they were not secured. The facility is currently working on identifying the number of affected individuals (the number could be between 350 - 5000), as well as identifying the identity of the potentially affected individuals.

ISO update: The ISO met again with local Incident Response Team. The team is still working on narrowing down the list of names using the method detailed below.
Patient cohort definition and filtering processes:
-- Original search performed for data range 10/13/10 to 05/20/14
-- Search criteria included all patients with a CPRS consult named "PFT (OUPT)" requested for the Denver division only
-- Within this criteria we identified consults with a status of "Completed" or "Partial Result"
-- Developed and compiled a list of patients where the PFT results that were actually performed on a device other that the portable laptop.
-- Compared and removed all patients where the PFT was physically performed on a device other than the portable laptop
-- Developed and compiled a Fileman report to identify any patient that had a manual scanned image stored within the Vista Imaging electronic records.

-- Filtered the results of the scanned images to exclude any C&P scanned records as these were performed at a different location
-- All duplicate records were removed
-- The final patients have been provided to the clinical staff for individual chart reviews

05/23/14:
Update: Based on the filtering processes below completed by the facility, there were 570 patients.

- 180 were the ones that had both an electronic result from the main system and also had another PFT order sent so it could not eliminate these from the original cohort as there was not a clean line saying it was only done on the main system. 100% audited; 155 names verified and will be removed. 180 - 155 = 25 (this number of patients will remain on the list)
- The remaining 390 patients, Service is still conducting a 100% audit; 176 more records to go.
- 570 - 155 = 415 may be affected. This is not the final number.

The team will meet again at 3:30 PM and the ISO send an update after the meeting.

ISO update: The ISO met again with Eastern Colorado Healthcare System (ECHCS) Facility Incident Response Team, 05/23/14, 3:00 PM local. This was confirmed by the team, there were 239 patients contained on the two stolen VA unencrypted laptops. The laptops contained personally identifiable information on the hard drives; full name, full Social Security number, birth dates, race, and test results.

05/27/14:
The ECHCS facility Incident Response Team has finished reviewing the information that could have been contained on the two missing laptops. The team has determined that 239 individuals' personally identifiable information (PII)/protected health information (PHI) would have been stored on the laptops.

Resolution

This incident was reported to OIG.

As per PO: The letters were mailed out on 05/29/14, a redacted credit-monitoring letter was uploaded, the employees in the department have retaken privacy/information security training, and the incident resolution column was updated.

DBCT **DBCT Decision Date:** 05/27/2014

05/27/14:
The DBCT has determined that 239 individuals will receive letters offering credit protection services.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000104474	Missing/Stolen Material (Non-Equipment)	VISN 10 Chillicothe, OH	5/22/2014		

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
VANSOC0606240	5/22/2014	INC000000370899 Category 1 -	N/A	N/A	N/A		

Incident Summary

During an IT Inventory, the facility was unable to locate two desktop workstations. Both are Win-7 operating systems and are encrypted. No sensitive data was stored on the PCs. A Report of Survey on both items was initiated by local OIT and forwarded to Logistics

Incident Update

05/22/14:
The Incident Resolution Service Team has determined that no data breach has occurred. The PCs are encrypted.

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 was a total of 1 IT Equipment Inventory Incident this reporting period.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000104642	Mishandled/ Misused Physical or Verbal Information	VISN 11 Battle Creek, MI	5/28/2014		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
VANSOC0606409	5/28/2014	INC000000372048 Category 4- Improper	N/A	N/A	N/A		

Incident Summary

A Veteran was informed that his/her VA ID Card and Medicare Card with full SSN was on Facebook. The Veteran stated that he/she does not use Facebook and did not know how the information had been placed on Facebook. The Privacy Officer (PO) walked the Veteran through Facebook to have the picture of Medicare Card and VA Card deleted. The card with SSN showing was being used as the Veteran's profile picture. The concern remains because the facility still has an ongoing investigation of possible stolen Veteran information.

Incident Update

06/04/14:
The full SSN was only on the Medicare card, which was displayed on Facebook. One of his friends emailed him to tell him that his Medicare card and VA ID were on his Facebook page and displayed as his pictures. With the PO's help, he was able to delete the image. This indicates that he must have previously set up the page. He stated that he probably set up the page back in 2010; however, was never prompted to enter a username and password.

06/10/14:
The Veteran still has his VA ID and Medicare card. The only way someone could have posted them to Facebook was to make a copy of them and upload the document. Looking at the Facebook account, it appears that the cards were copied and the piece of paper uploaded as a photo.

Resolution

The Privacy Officer helped the Veteran remove the images of the Medicare and VA ID cards from Facebook and also has sent a message to the Facebook Privacy Office to have the account reported as hacked, as the Veteran stated they did not know about this or ever had heard of the high school that was listed. The only other mitigation would be to offer credit monitoring, as the Veteran's full SSN was posted for public viewing.

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

06/03/14:
The DBCT wanted to know if the SSN was on the VA ID or just on the Medicare card, how did the Veteran know the information was on Facebook and how was he able to edit the page. Questions sent to the PO.

06/10/14:
The DBCT would like to know if he still has his VA ID and Medicare card.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened		Date of Initial DBCT Review
PSETS0000104713	Mishandled/ Misused Physical or Verbal Information	VISN 08 San Juan, PR	5/29/2014	Date Closed	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
VANSOC0606476	5/29/2014	INC000000372414 Category 6 -	N/A	N/A	N/A		

Incident Summary

While performing an Environment of Care (EOC) rounds in the new Mayaguez Outpatient Clinic, the Information Security Officer (ISO) found lots of paper documents in the dumpster. These documents were dated from 1995 to 1998.

Incident Update

06/03/14:
There are various documents regarding information on 83 Veterans and three employees. All include the full name and full SSN. Some were contained in clear plastic bags and some were laying loose in and around the dumpster. The dumpster is located in the parking lot of the clinic and accessible to the public. It is not known how long the documents were in the dumpster.

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

Based on the opinion of the Privacy Officer and the pictures provided, the DBCT believes that credit protection services should be offered. Video of the area should be reviewed prior to making notification. This is a new clinic and few people are familiar with the security system. The Privacy Officer is waiting on one Police Officer to review the cameras.

Total number of Internal Un-encrypted E-mail Incidents	97
Total number of Mis-Handling Incidents	120
Total number of Mis-Mailed Incidents	159
Total number of Mis-Mailed CMOP Incidents	1
Total number of IT Equipment Inventory Incidents	1
Total number of Missing/Stolen PC Incidents	2 (0 encrypted)
Total number of Missing/Stolen Laptop Incidents	2 (0 encrypted)
Total number of Lost BlackBerry Incidents	24
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	1