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



Monthly Report to Congress of Data Incidents
June 30 - August 3, 2014

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review		
PSETS0000106008	Mishandled/ Misused Physical or Verbal Information	VISN 10 Chillicothe, OH	7/1/2014	7/21/2014			
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
VANSOC0607706	7/1/2014	INC000000380416 Category 6 -	N/A	N/A	N/A		1
Incident Summary A clinic clerk mailed lab results that belonged to Veteran B to Veteran A. Veteran A, who received the results, contacted the clinic and returned the document.							
Incident Update 07/01/14: 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 Community Based Outpatient Clinic manager met with employee who was responsible for mailing lab results to the wrong Veteran. The process was reviewed to prevent similar incidents from occurring in the future.							
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 160 Mis-Mailed incidents this reporting period. Because of repetition, the other 159 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		
PSETS0000106022	Non-VA Responsible/Non-Incident Upon Further	VISN 20 Roseburg, OR	7/1/2014	7/31/2014			
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
VANSOC0607722	7/1/2014	INC000000380493 Category 1 -	N/A	N/A	N/A		
Incident Summary							
<p>An IT employee signed for equipment and noticed a laptop was missing. She contacted the warehouse to let them know that she only had two of the three laptops. On 02/19/14, the employee also sent an email documenting the fact that IT was not in possession of this equipment. The IT manager followed up with an email to logistics on 05/27/14 and again on 06/24/14. All IT areas were searched, including A319A where the other laptops were delivered. This search included all desks, cabinets and storage areas. Additionally, the entire facility had a contracted wall to wall equipment inventory the last two weeks of May where all IT and non-IT equipment was scanned for inventory purposes. This laptop was not scanned into the IT storage area or any other area and IT staff cannot confirm they were ever in possession of this laptop. From an information security standpoint, this laptop was never imaged or placed on the VA Network. There is no possibility of this equipment having VA or patient information on it. Property and warehouse staff searched the warehouse again for the missing item, but it was not found.</p>							
Incident Update							
<p>07/01/14: The Incident Resolution Service Team has determined that no data breach has occurred. The laptop was never imaged, had never connected to the VA network, and had never stored any VA information.</p>							
Resolution							
<p>Due to the fact that the laptop was never configured or used on a VA Network, this incident can be closed. A report of survey has been made and handed over to the VA Police.</p>							
DBCT							
<p>DBCT Decision Date: N/A</p> <p>No DBCT decision is required. This stays on as informational for missing equipment.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review		
PSETS0000106047	Mishandled/ Misused Physical or Verbal Information	VISN 20 Portland, OR	7/1/2014				
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
VANSOC0607747	7/1/2014	INC000000380607 Category 6 -	N/A	N/A	N/A		1
Incident Summary							
As Veteran A was leaving his eye appointment on 06/26/14, the VA clerk checking him out scheduled a follow-up appointment for 07/07/14 but selected Veteran B's record by mistake. A reminder letter was printed and given to Veteran A for the upcoming appointment. This was discovered by Veteran A who called the next day to notify the facility of the error. The schedule was corrected and the Veteran will be returning the letter to the facility when he comes in for his next appointment. The letter he received contained Veteran B's full name, mailing address, and the last four of his SSN.							
Incident Update							
07/02/14: 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.							
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 128 Mis-Handling incidents this reporting period. Because of repetition, the other 127 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		
PSETS0000106426	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Charleston, SC	7/11/2014	7/15/2014			
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
VANSOC0608130	7/11/2014	INC000000382826 Category 6 -	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 Charleston VA Medical Center (station 534) and a replacement has been requested for Patient B. The Charleston Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error.							
Incident Update							
07/11/14: 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							
On 7/11/14, 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 9 Mis-Mailed CMOP incidents out of 7,825,920 total packages (11,526,561 total prescriptions) mailed out for this reporting period. Because of repetition, the other 8 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		
PSETS0000106787	Missing/Stolen Equipment	VISN 07 Montgomery, AL	7/21/2014				
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
VANSOC0608486	7/21/2014	INC000000385012 Category 1 -	N/A	N/A	N/A		
Incident Summary During an annual IT inventory check, ten desktop computers and one laptop computer were discovered as missing.							
Incident Update 07/21/14: The ten desktops and one laptop are all encrypted. The laptop was last seen in June 2013, which is also when it was last connected to the network. This was not reported to the VA Police because it is believed that this is an inventory tracking issue and not a theft. 08/11/14: IT staff is still inventorying and looking for the missing items. A Report of Survey is being completed.							
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 8 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 7 is 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		
PSETS0000106927	Mishandled/ Misused Physical or Verbal Information	VISN 07 Columbia, SC	7/23/2014		7/29/2014		
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
VANSOC0608608	7/23/2014	INC000000385628 Category 6 -	N/A	N/A	N/A	2179	1458
<p>Incident Summary A VA Employee (Service Line Records Liaison) noticed on 07/14/14 that four boxes that were being prepared for shipment to the Records Center and Vault located in Neosho, Missouri, were missing. The four boxes were labeled with Accession #VHA-14-0797 for long term storage. According to the Records Liaison, the boxes were kept behind keypad locked doors; however some of the boxes were moved into the morgue hallway from the locked room without her knowledge.</p> <p>VA Police, Privacy Officer, Records Manager, and OIG special agents were notified. A walk-through of last known area(s) was conducted. A VA Police Investigator, Records Manager, OIG special agents, and ISO conducted a walk-through and inspection of the temporary onsite storage facility. The Records Liaison and Records Manager conducted a thorough search of all other packaged boxes (69) and accounted for each file in each accession. All files accounted for except four boxes missing in question.</p>							
<p>Incident Update</p> <p>07/22/14: The records have not been located. They are in four boxes. Each sheet of paper in the boxes is on a separate Veteran. There is a total of 3,637 Veterans involved. No cameras are in the area. Engineering was doing work in the area and the doors were unlocked when it was determined that the four boxes were missing.</p> <p>07/29/14: The DBCT has determined that credit protection services will be offered to all Veterans involved in this incident. A next of kin (NOK) notification letter will be sent if the Veteran is deceased.</p> <p>08/07/14: The total number of Veterans that will be offered credit protection services is 2,179. The remaining 1,458 will receive NOK letters.</p>							
<p>DBCT DBCT Decision Date: 07/29/2014</p> <p>The DBCT has determined that credit protection services will be offered to all Veterans involved in this incident. A next of kin letter will be sent if the Veteran is deceased.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review		
PSETS0000107332	Mishandled/ Misused Physical or Verbal Information	VISN 18 Albuquerque, NM	8/1/2014		8/5/2014		
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
VANSOC0609116	8/1/2014	INC000000388046 Category 6 -	8/1/2014	Yes	Pending	2670	

Incident Summary

A folder containing multiple patients' information including full names, SSN's, and other medical information was found in a ladies restroom on the first floor of Bldg. 41 and brought to the Chief Records Manager. A preliminary review of the folder by the Records Manager indicated there were 3,463 patients' information contained in this folder and 3,427 full patients' SSNs. There is evidence to suggest this folder belonged to one of the release of information (ROI) clerks. The Records Manager was going to be meeting with the employee who allegedly misplaced the information on 08/01/14.

Incident Update

08/01/14:

The Privacy Officer reports that this was found in a public restroom in one of the main lobby areas of the medical center. It was found at approximately 4:00 PM on 07/30/14. At this point of the investigation, the documents are believed to have been left in the restroom for less than two hours. The folder was left by a VA employee who was scheduled to have a meeting with HR and union officials. It appears that the document containing the patient names and SSNs was printed to show the employee's workload. The majority of the names and SSNs were on this ROI workload report. The report columns on the listing were: patient name, SSN, first or third party request, and status of request. Approximately 80 ROI request forms were also in the folder, which contain the patient name, date of birth, SSN, and what information was being requested, which could be clinical information. When questioning the employee about the folder, the employee stated that she had been storing the information in the trunk of her car, but changed that story later in the interview to say that she never took it off VA grounds. The Privacy Officer and Chief of HIMS are continuing to investigate the incident. This will be discussed during the 08/05/14 DBCT meeting.

08/05/14:

The DBCT determined that since the information was left unattended in a public area of the Medical Center for approximately two hours during the work day, that there is a risk of data breach. All Veterans whose SSNs were disclosed in the file will be offered credit protection services. This is a HITECH Act reportable breach. The Privacy Officer is researching the other 36 patients who did not have their SSN disclosed to see what information was disclosed on them. At this point 3,427 Veterans will be offered credit protection services, and a press release will be required.

08/07/14:

The PO has revised the total number of individuals affected to 2,670 after duplicates were removed.

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

08/05/14:
The DBCT determined that since the information was left unattended in a public area of the Medical Center for approximately two hours during the work day, that there is more than a low risk of a data breach. All Veterans whose SSN was disclosed in the file will be offered credit protection services. This is a HITECH Act reportable breach.

Total number of Internal Un-encrypted E-mail Incidents	115
Total number of Mis-Handling Incidents	128
Total number of Mis-Mailed Incidents	160
Total number of Mis-Mailed CMOP Incidents	9
Total number of IT Equipment Inventory Incidents	8
Total number of Missing/Stolen PC Incidents	1 (1 encrypted)
Total number of Missing/Stolen Laptop Incidents	9 (8 encrypted)
Total number of Lost BlackBerry Incidents	20
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	1