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



Monthly Report to Congress of Data Incidents
March 31 - May 4, 2014

Security Privacy Ticket Number		Incident Type		Organization		Date Opened		Date Closed		Date of Initial DBCT Review					
PSETS0000102143		Mishandled/ Misused Physical or Verbal Information		VBA Atlanta, GA		3/31/2014		4/3/2014							
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	
VANSOC0603981		3/31/2014		INC0000000357506 Category 6 -		N/A		N/A		N/A		1			
Incident Summary Veteran A entered the Veteran Service Organization with documents belonging to Veteran B. Veteran A stated the documents belonging to Veteran B were attached to his VA correspondence letter. The Veteran Service Organization mailed the copies back to the Regional Office. Veteran B's name, address, and full SSN were compromised.															
Incident Update 03/31/14: The Incident Resolution Team has determined that Veteran B will be sent a letter offering credit protection services due to his full SSN being compromised.															
Resolution The employee was counseled by the supervisor on the importance of identifying specific records sent to Veterans. The employee was also counseled on the proper way to release letters to Veterans or beneficiaries prior to mailing in order to prevent a personally identifiable information (PII) violation from occurring.															
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 199 Mis-Mailed incidents this reporting period. Because of repetition, the other 198 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
PSETS0000102170		Mishandled/ Misused Physical or Verbal Information	VISN 20 Roseburg, OR		3/31/2014	4/17/2014	
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
VANSOC0604008	3/31/2014	INC000000357656 Category 6 -	N/A	N/A	N/A	1	
Incident Summary A medication list for Veteran A was sent home with Veteran B. Veteran A's name, full SSN, date of birth and medication information were compromised.							
Incident Update 03/31/14: The Incident Resolution Team has determined that Veteran A will be sent a letter offering credit protection services due to the full SSN being compromised.							
Resolution The processes have been updated. The credit monitoring letter was sent on 04/17/14.							
DBCT <div>DBCT Decision Date: N/A</div> <p>No DBCT decision is required. This is informational for Mis-Handling incidents and is the representative ticket. There were a total of 122 Mis-Handling incidents this reporting period. Because of repetition, the other 121 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.</p>							

Security Privacy Ticket Number		Incident Type	Organization		Date Opened	Date Closed		Date of Initial DBCT Review
PSETS0000102244		Missing/Stolen Equipment	VISN 23 Iowa City, IA		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	
VANSOC0604078	4/1/2014	INC000000358381 Category 6 -	N/A	N/A	N/A			
Incident Summary During a routine inventory of VA imaging equipment, it was discovered that four devices capable of storing VA data could not be located. Three are Personal Computers and one is a Western Digital USB Drive. No determination has been made if the devices were encrypted or the kind of data the devices supported. The inventory list states the devices may have been transferred to another VA without proper documentation. A Report of Survey has been submitted to Logistics and the VA Police have been notified.								
Incident Update 04/11/14: This is still under investigation of the VA Police. 05/02/14: There is no new information at this time.								
DBCT No DBCT decision is required. This is informational for IT Equipment Inventory incidents and is the representative ticket. There were a total of 7 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 6 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		
PSETS0000102487	Mishandled/ Misused Physical or Verbal Information	VISN 02 Buffalo, NY	4/7/2014	5/5/2014			
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
VANSOC0604309	4/7/2014	INC0000000359565 Category 6 -	N/A	N/A	N/A		82
Incident Summary IT staff found a gains and losses sheet for 04/04/14 in the kiosk next to the canteen store. She secured the list and brought it to the Privacy Officer (PO). The list contains 82 Veterans' full name, last 4 digits of the SSN and the ward they were admitted to or discharged from.							
Incident Update 04/07/14: Per the PO, the list was printed 04/05/14, and found 04/07/14 at approximately 7:30 AM. The PO is checking to see if there are any cameras in the area. 04/08/14: Per the PO, there are no cameras in area. Due to the fact that it was left unattended for 2 days in a public area, the Incident Resolution Team (IRT) has determined that eighty-two Veterans will be sent a HIPAA notification letter due to Protected Health Information (PHI) being exposed.							
Resolution The HIPAA notification letters mailed 05/05/14. The PO is unable to determine who dropped the list. General education was provided to the entire staff on 05/05/14.							
DBCT <div style="float: right;">DBCT Decision Date: N/A</div> 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					
PSETS0000102498		Mishandled/ Misused Physical or Verbal Information		VHA CMOP Charleston, SC		4/7/2014		4/10/2014							
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	
VANSOC0604320		4/7/2014		INC000000359625 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 medical center and a replacement has been requested for Patient B. Charleston 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 04/07/14: 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 On 3/26/14, the CMOP employee was counseled and retrained in proper packing procedures.															
DBCT <div>DBCT Decision Date: N/A</div> 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 8,070,233 total packages (11,777,227 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		
PSETS0000103009	Missing/Stolen Equipment	VISN 07 Charleston, SC	4/17/2014	4/28/2014			
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
VANSOC0604815	4/17/2014	INC000000362777 Category 1 -	N/A	N/A	N/A		
Incident Summary The Information Security Officer (ISO) was informed by VA Police that the Customer Service Representative reported two computers missing from the facility. The computers were EE174496 and EE174497. The computers were used for Veterans and family members in the waiting rooms. The computers contain no personally identifiable information (PII) or protected health information (PHI). The two devices are still missing but an investigation is still in progress.							
Incident Update 04/18/17: The PCs were used for public access and did not contain any information. No breach occurred.							
Resolution Locking chains will be placed on the devices the next time and the devices will be monitored.							
DBCT <div style="text-align: right;">DBCT Decision Date: N/A</div> 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	
PSETS0000103026		Mishandled/ Misused Physical or Verbal Information		VISN 06 Salisbury, NC		4/18/2014					
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	
VANSOC0604835	4/18/2014	INC000000363215 Category 6 -		N/A	N/A	N/A		182			
Incident Summary There are 182 travel vouchers missing that contain Veterans' names, full SSNs, and other information. The facility received a multitude of phone calls from Veterans requesting payment for vouchers they placed in a box on 03/11/14 from one of our facility Community Based Outpatient Clinics (CBOC). The vouchers are transported from the CBOC to the medical center by mail courier, however no vouchers from 03/11/14 can be located in the Fiscal Department from the CBOC. When the mail courier is off the travel vouchers are transported by facility warehouse staff. The travel vouchers have not been found in the facility warehouse.											
Incident Update 04/18/14: The Incident Resolution Team has determined that 182 Veterans will be sent letters offering credit protection services, as documents containing their full SSNs have been lost.											
DBCT <div>DBCT Decision Date: N/A</div> <div>No DBCT decision needed. This is informational due to the number of Veterans affected.</div>											

Security Privacy Ticket Number		Incident Type		Organization		Date Opened		Date Closed		Date of Initial DBCT Review	
PSETS0000103503		Missing/Stolen Equipment		EMPLOYEE EDUCATION SERVICE/ EES St. Louis, MO		4/30/2014				5/6/2014	
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	
VANSOC0605316	4/30/2014	INC000000365979 Category 1 -		N/A	N/A	N/A					
Incident Summary On 04/24/14, local IT staff notified the backup Information Security Officer (ISO) that as part of IT inventory, 6 laptops were missing from their inventory. The backup ISO notified the National Service Desk (NSD) who created NSD ticket #R2715331FY14. These laptops were stored on VA premises in a fenced locked caged area. IT staff stated the hard drives were removed from the laptops as part of the media sanitization process. The backup ISO contacted the VA Police and made them aware of the situation. The ISO is attaching a completed Report of Survey (ROS).											
Incident Update 04/30/14: The 6 laptops are missing as part of VA inventory. They were last located on VA premises in the fenced locked caged area. They were all seen within the last six months. The laptops were encrypted and the hard drives were removed before they were placed in the cage. Each of these systems was being processed to be excessed/turn-in items. They were collected, removed from AD, drives pulled/destroyed and processed for excessing and stored in secured caged area. The Employee Education Service (EES) does not work with Veteran or patient health information. They instruct their users to store any personally identifiable information (PII) related to employees on the secure network drive and not on the computer hard drive. 05/05/14: EES will forward the ROS to VAMC Police who will in turn assign an investigator, perform the investigation and then provide EES with a copy of the Police report and number.											
DBCT No DBCT decision needed. This stays on as informational for missing equipment.											
DBCT Decision Date: N/A											

Total number of Internal Un-encrypted E-mail Incidents	111
Total number of Mis-Handling Incidents	122
Total number of Mis-Mailed Incidents	199
Total number of Mis-Mailed CMOP Incidents	9
Total number of IT Equipment Inventory Incidents	7
Total number of Missing/Stolen PC Incidents	9
Total number of Missing/Stolen Laptop Incidents	12 (10 encrypted)
Total number of Lost BlackBerry Incidents	22
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	1