

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

Monthly Report to Congress of Data Incidents
September 1-30, 2014

Security Privacy Ticket Number: PSETS0000108600
Incident Type: Mishandled/ Misused Physical or Verbal Information
Organization: VISN 01
Boston, MA
Date Opened: 9/2/2014
Date Closed:
Date of Initial DBCT Review: 9/9/2014
VA-NSOC Incident Number: VANSOC0610365
Date US-CERT Notified: 9/2/2014
US-CERT Case Number: INC000000396435
US-CERT Category: Category 6 - Investigation
No. of Credit Monitoring: 282
No. of Loss Notifications:
DBCT Category: Mishandling

Incident Summary

Information was found on a printer that is in a public area with no VA Police security camera on it. It was printed the morning of 8/29 at 7:47AM. It included fifty-six pages of patient clinic lists for the following clinics: dermatology, dialysis, mental health, eye, ears nose and throat, GI, pain, anesthesia, dental, and audiology.

Incident Update

09/04/14:

The area was locked from the evening of Friday 8/29/14 through the morning of Tuesday 9/2/14, however there are several hours on Friday where the information was accessible.

09/12/14:

All 293 Veterans will receive letters offering credit protection services due to full SSN being potentially accessible.

09/15/14:

After duplicates were found, the total is 282 Veterans affected.

DBCT Decision Date: 09/09/2014

DBCT

09/09/14:

The DBCT determined that due to the length of time the information was unattended and that there were no cameras or ways to verify the information was not accessed, credit protection services are warranted.

Security Privacy Ticket Number: PSETS0000108616
Incident Type: Mishandled/ Misused Physical or Verbal Information
Organization: VISN 09
Louisville, KY
Date Opened: 9/2/2014
Date Closed: 10/2/2014
Date of Initial DBCT Review: 9/9/2014
VA-NSOC Incident Number: VANSOC0610380
Date US-CERT Notified: 9/2/2014
US-CERT Case Number: INC000000396512
US-CERT Category: Category 6 - Investigation
No. of Credit Monitoring:
No. of Loss Notifications: 200
DBCT Category: Mishandling

Incident Summary

A dermatology physician self-reported that his car was broken into over the weekend of August 30-31. His white coat was stolen which had a listing of approximately 200 Veterans with their full name, last four numbers of their SSN, diagnosis, biopsy location and pathology notes.

Incident Update

09/02/14:
The physician is a contract physician who works for the University of Louisville. The clinic is at the VA location and the contracted physicians come to the VA to see patients in the clinic.

09/12/14:
All 200 Veterans will receive HIPAA notification letters due to protected health information being exposed.

Resolution

The Privacy Officer met with clinical leadership and spoke at length regarding the safeguarding of information. She also discussed students and residents not taking information off VA property unless properly authorized to do so. The Privacy Officer noted that an electronic spreadsheet could be utilized in tracking this information for patients. This incident resulted in publishing a bulletin in regards to carrying information off station.

DBCT Decision Date: 09/09/2014

DBCT

09/09/14:
The DBCT decided that this will require 200 HIPAA notification letters.

Security Privacy Ticket Number: PSETS0000108629
Incident Type: Mishandled/ Misused Physical or Verbal Information
Organization: VBA
Oakland, CA
Date Opened: 9/2/2014
Date Closed:
Date of Initial DBCT Review: N/A
VA-NSOC Incident Number: VANSOC0610399
Date US-CERT Notified: 9/2/2014
US-CERT Case Number: INC000000396552
US-CERT Category: Category 6 - Investigation
No. of Credit Monitoring: 1
No. of Loss Notifications:
DBCT Category: Mismatched

Incident Summary

Veteran A received a letter from the Oakland Regional Office (RO) and in the same envelope was a letter meant for Veteran B. Veteran A sent the letter to his Congressman, who forwarded it to the RO, where it was referred to the Privacy Officer. The letter included Veteran B's full name and SSN

Incident Update

09/03/14:

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

DBCT Decision Date: N/A

DBCT

No DBCT decision is required. This is informational for Mis-Mailed incidents and is the representative ticket. There were a total of 157 Mis-Mailed incidents this reporting period. Because of repetition, the other 156 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: PSETS0000108726
Incident Type: Mishandled/ Misused Physical or Verbal Information
Organization: VISN 17
San Antonio, TX
Date Opened: 9/4/2014
Date Closed: 9/11/2014
Date of Initial DBCT Review: N/A
VA-NSOC Incident Number: VANSOC0610493
Date US-CERT Notified: 9/4/2014
US-CERT Case Number: INC000000397265
US-CERT Category: Category 6 - Investigation
No. of Credit Monitoring: 1
No. of Loss Notifications:
DBCT Category: Mishandling

Incident Summary

The Emergency Department gave paperwork (medication reconciliation) to the wrong Veteran. The error was caught during the patient identification process at the Pharmacy window and taken from the patient.

Incident Update

09/04/14:

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

Resolution

Staff was re-educated on 09/04/14.

DBCT Decision Date: N/A

DBCT

No DBCT decision is required. This is informational for Mis-Handling incidents and is the representative ticket. There were a total of 105 Mis-Handling incidents this reporting period. Because of repetition, the other 104 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: PSETS0000108856
Incident Type: Missing/Stolen Equipment
Organization: VISN 02
Albany, NY
Date Opened: 9/8/2014
Date Closed: 9/10/2014
Date of Initial DBCT Review: 9/16/2014
VA-NSOC Incident Number: VANSOC0610667
Date US-CERT Notified: 9/8/2014
US-CERT Case Number: INC000000398235
US-CERT Category: Category 1 - Unauthorized Access
No. of Credit Monitoring:
No. of Loss Notifications:
DBCT Category: Lost Non-Blackberry Mobile
Devices

Incident Summary

It was reported to the Information Security Officer that two Environment of Care (EOC) tablet computers are missing. The tablets were signed for in Logistics in May. The tablets were never received in the IT section. The Chief Information Officer has stated that the tablets have no VA image or data on them. A police report is being filed at this time.

Incident Update

09/09/14:

The tablets are Fujitsu Stylistic Q572 Tablets. IT installs the encryption software and since the tablets never made it to IT and they have no VA image (or data), they were not encrypted. The Incident Resolution Team has determined that no data breach has occurred.

Resolution

Logistics has been educated on the importance of tracking equipment more carefully.

DBCT Decision Date: 09/16/2014

DBCT

No DBCT decision is required. This stays on the report as informational for missing equipment.

Security Privacy Ticket Number: PSETS0000108867
Incident Type: Missing/Stolen Equipment
Organization: VISN 20
Seattle, WA
Date Opened: 9/8/2014
Date Closed: 9/24/2014
Date of Initial DBCT Review: N/A
VA-NSOC Incident Number: VANSOC0610679
Date US-CERT Notified: 9/8/2014
US-CERT Case Number: INC000000398281
US-CERT Category: Category 1 - Unauthorized Access
No. of Credit Monitoring:
No. of Loss Notifications:
DBCT Category: Unencrypted iPad Stolen

Incident Summary

A Utilization Nurse noticed on the morning of 09/08/14 that his VA Mobile Health Deployment iPad had been stolen from his desk. The office space had recently been cleaned and painted but his interior office had been locked. The iPad had not been used except minimally as the nurse was waiting for the application he needs to be approved and loaded. There was a PIN in use and the iPad was locked and actually turned off (as it was effectively in storage). This was reported to the VA police and they are coordinating with city police as the GPS tracking shows where the device was taken (off campus). There is no data residing on the tablet itself.

Incident Update

09/09/14:

The Incident Resolution Service Team has determined that no data breach occurred, as there was no VA data stored on the iPad.

Resolution

The helpdesk was notified and the wipe device command has been initiated. The iPad is currently off and the wipe device command will not take effect until the machine is turned back on.

DBCT Decision Date: N/A

DBCT

No DBCT decision is required. This stays on as informational for missing equipment.

Security Privacy Ticket Number: PSETS0000108902
Incident Type: Missing/Stolen Equipment
Organization: VISN 03
Montrose, NY
Date Opened: 9/9/2014
Date Closed: 9/11/2014
Date of Initial DBCT Review: 9/16/2014
VA-NSOC Incident Number: VANSOC0610715
Date US-CERT Notified: 9/9/2014
US-CERT Case Number: INC000000398543
US-CERT Category: Category 1 - Unauthorized Access
No. of Credit Monitoring:
No. of Loss Notifications:
DBCT Category: IT Equipment Inventory

Incident Summary

A Report of Survey was issued for the fiscal year 2014 information technology inventory which identified 12 PC's that cannot be located.

Incident Update

09/09/14:
The Incident Resolution Service Team has determined that no data breach has occurred. The twelve PCs were encrypted, additionally the PCs were installed with Scriptlogic which prevents saving data to the local drive.

Resolution

All 12 CPU's which were reported missing during the FY 14 final inventory contained hard drives that were encrypted and also were protected by Script Logic. Please close this ticket.

DBCT Decision Date: 09/16/2014

DBCT

No DBCT decision is required. This is informational as an IT equipment inventory incident. This was the only IT equipment inventory incident during the reporting period.

Security Privacy Ticket Number: PSETS0000109292
Incident Type: Mishandled/ Misused Physical or Verbal Information
Organization: VISN 17
San Antonio, TX
Date Opened: 9/18/2014
Date Closed: 10/9/2014
Date of Initial DBCT Review: 9/23/2014
VA-NSOC Incident Number: VANSOC0611094
Date US-CERT Notified: 9/18/2014
US-CERT Case Number: INC000000401395
US-CERT Category: Category 6 - Investigation
No. of Credit Monitoring:
No. of Loss Notifications: 4000
DBCT Category: Mismailed

Incident Summary

On September 15, 2014, a Veterans Health Administration New Federal Rule of Hydrocodone Combination Products information letter was mailed to approximately 4,000 Veterans. On September 17, 2014, the Privacy Office was notified the letters mailed were printed double-sided, which means only 2,000 letters were mailed, with another Veterans name/information printed on the other side. VA cannot determine which Veterans information was disclosed out of the 4,000 letters mailed. The letters were folded and stuffed in the envelopes, so there is no way to determine who received the letters and who did not. The information breached is full name, address, and that the patient is currently prescribe a Hydrocodone product.

Incident Update

09/18/14:

The Incident Resolution Service Team has determined that 4000 Veterans will be sent HIPAA notification letters due to Protected Health Information (PHI) being potentially disclosed.

10/07/14:

The letters were mailed on October 3, 2014. The press release is scheduled for October 8, 2014.

10/08/14:

The press release was done on October 8, 2014.

Resolution

All individuals involved were re-educated on the importance of checking documents at time of printing and prior to stuffing envelopes. Training occurred between September 22nd and 23rd.

DBCT Decision Date: 09/23/2014

DBCT

The DBCT concurred that this is a data breach. It involves over 500 Veterans and is a HITECH Act breach, which will require a press release.

Security Privacy Ticket Number: PSETS0000109470
Incident Type: Mishandled/ Misused Physical or Verbal Information
Organization: VHA CMOP
Dallas, TX
Date Opened: 9/23/2014
Date Closed: 9/25/2014
Date of Initial DBCT Review: N/A
VA-NSOC Incident Number: VANSOC0611322
Date US-CERT Notified: 9/23/2014
US-CERT Case Number: INC000000402612
US-CERT Category: Category 6 - Investigation
No. of Credit Monitoring:
No. of Loss Notifications: 1
DBCT Category: CMOP Mismatched

Incident Summary

Patient A received a Medline Industries medical supply intended for Patient B. Patient B's name and type of medical supply was compromised. Patient A reported the incident to the Muskogee VA Medical Center and a replacement has been requested for Patient B. Dallas Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a Medline packing error. The packing error has been reported to Medline for investigation and corrective action.

Incident Update

09/23/14:

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

Resolution

On 9/23/14, the packing error was reported to Medline for investigation and corrective action.

DBCT Decision Date: N/A

DBCT

No DBCT decision is required. This is informational for Mis-Mailed CMOP incidents and is the representative ticket. There were a total of 4 Mis-Mailed CMOP incidents out of 7,274,779 total packages (10,426,432 total prescriptions) mailed out for this reporting period. Because of repetition, the other 3 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: PSETS0000109683
Incident Type: Mishandled/ Misused Physical or Verbal Information
Organization: VISN 10
Cincinnati, OH
Date Opened: 9/26/2014
Date Closed:
Date of Initial DBCT Review: N/A
VA-NSOC Incident Number: VANSOC0611486
Date US-CERT Notified: 9/26/2014
US-CERT Case Number: INC000000403667
US-CERT Category: Category 6 - Investigation
No. of Credit Monitoring: 90
No. of Loss Notifications:
DBCT Category: Mismatched

Incident Summary

A UPS package containing personally identifiable information and protected health information of a Veteran was mailed to the Veteran's home address. When the Veteran opened the package and noticed there were other Veterans' documents inside, they called VHA and informed the staff of the mistake. The Veteran then delivered the package to the medical center and left the package opened on the receptionist desk at 7:45 AM on 09/26/14. The UPS package was then noticed by the Supervisor at 8:00 AM on 9/26/14.

Incident Update

09/26/14:
The Incident Resolution Service Team has determined that Veterans whose information was disclosed will be sent a letter offering credit protection services.

09/30/14:
The facility has determined that there was ninety Veterans' information on the documents.

DBCT Decision Date: N/A

DBCT

No DBCT decision was required. This is left on the report as informational due to the number of Veterans involved.

Security Privacy Ticket Number: PSETS0000109844
Incident Type: Missing/Stolen Equipment
Organization: VISN 23
Minneapolis, MN
Date Opened: 9/30/2014
Date Closed: 10/2/2014
Date of Initial DBCT Review: 10/7/2014
VA-NSOC Incident Number: VANSOC0611643
Date US-CERT Notified: 9/30/2014
US-CERT Case Number: INC000000404829
US-CERT Category: Category 1 - Unauthorized Access
No. of Credit Monitoring:
No. of Loss Notifications:
DBCT Category: Unencrypted Laptop Missing

Incident Summary

An Apple laptop used by a Minneapolis researcher was identified as missing as part of the inventory process. The researcher had not reported the loss. The laptop is not encrypted.

Incident Update

10/02/14:

The laptop was purchased with Research (VA) grant dollars in 2006. It was designated as VA equipment placed on the Research equipment inventory list (EIL). There is no evidence to indicate that the laptop had been encrypted. Neither IT staff nor the Information Security Officers were aware of the existence of the laptop because it had not been processed through the current IT equipment purchasing process, which was not in use in 2006, and the laptop was on the Research inventory list. The laptop had apparently been used in the Researcher's home, not his office as previously reported. The loss was noted when he could not produce the laptop during a recent inventory.

The laptop appears to have been serviced by the Biomed Service within the medical center at times throughout its lifecycle. The Biomed Engineer that serviced it has since retired. The Researcher has been contacted and he provided the following information: the laptop was purchased years ago with research funds and was never used in the medical center; it was to be used to write grants and papers and remained at the researcher's home; the laptop was never encrypted and did not contain any sensitive data such as protected health information or personally identifiable information; the computer was never connected to the VA network; unfortunately, the laptop overheated one year ago, and it was brought to the First Tech store in Uptown. They advised destroying the computer because of battery leakage that could pose a danger. The computer was left with them and they assured the researcher that it would be disposed of responsibly.

The researcher stated again that there were no records whatsoever, of identifiers of Veterans or any other work related information contained on the laptop. A report of survey has been signed by the ACOS of Research and will be provided to the Police. The Incident Resolution Service Team has determined that this was a policy violation, as the destruction process was not completed correctly, but no data breach has occurred as the laptop did not contain VA data.

Resolution

The Researcher has reported that the laptop had been destroyed (not in accordance with VA requirements) and that the laptop did not contain PHI or PII. The Report of Survey has been signed by the ACOS of Research and will be provided to the Police.

DBCT Decision Date: 10/07/2014

DBCT

10/07/14:

The DBCT concurred that no data breach has occurred, since no VA data was on the device.

Total number of Internal Un-encrypted E-mail Incidents	88
Total number of Mis-Handling Incidents	105
Total number of Mis-Mailed Incidents	157
Total number of Mis-Mailed CMOP Incidents	4
Total number of IT Equipment Inventory Incidents	1
Total number of Missing/Stolen PC Incidents	0
Total number of Missing/Stolen Laptop Incidents	5 (4 encrypted)
Total number of Lost BlackBerry Incidents	26
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	4