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

**Monthly Report to Congress of Data Incidents**

**August 4-31, 2014**

| | |
|---|---|
| **ecurity Privacy Ticket Number:** | PSETS0000107501 |
| **ncident Type:** | Mishandled/ Misused Physical or Verbal Information |
| **Organization:** | VBA<br>Waco, TX |
| **Date Opened:** | 8/5/2014 |
| **Date Closed:** | 8/11/2014 |
| **Date of Initial DBCT Review:** | N/A |
| **/A-NSOC Incident Number:** | VANSOC0609279 |
| **Date US-CERT Notified:** | 8/5/2014 |
| **JS-CERT Case Number:** | INC000000389148 |
| **JS-CERT Category:** | Category 6 - Investigation |
| **No. of Credit Monitoring:** | 1 |
| **No. of Loss Notifications:** | |
| **DBCT Category:** | Mismailed |

**ncident Summary**

A letter was mailed to Veteran A that erroneously contained Veteran B's name, address, SSN, and medical condition.

**ncident Update**

08/06/14:
The Incident Resolution Service Team has determined that Veteran B will be sent a letter offering credit protection services.

**Resolution**

The employee will receive formal counseling and the Veteran has been sent a letter of explanation along with the offer for free credit monitoring.

**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 138 Mis-Mailed incidents this reporting period. Because of repetition, the other 137 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.

| | |
|---|---|
| **ecurity Privacy Ticket Number:** | PSETS0000107703 |
| **ncident Type:** | Mishandled/ Misused Physical or Verbal Information |
| **Organization:** | VBA<br>Cleveland, OH |
| **Date Opened:** | 8/11/2014 |
| **Date Closed:** | |
| **Date of Initial DBCT Review:** | 8/19/2014 |
| **/A-NSOC Incident Number:** | VANSOC0609469 |
| **Date US-CERT Notified:** | 8/11/2014 |
| **JS-CERT Case Number:** | INC000000390516 |
| **JS-CERT Category:** | Category 6 - Investigation |
| **No. of Credit Monitoring:** | 269 |
| **No. of Loss Notifications:** | |
| **DBCT Category:** | Mishandling |

**ncident Summary**

A call center agent in the National Call Center left a steno notebook in a common break area which was accessible to the public. The notebook ontained claim and social security numbers.

**ncident Update**

)8/11/14:
The Information Security Officer cannot determine how long the notebook was in the break area at this time. The notebook was found by a VA employee who is on the Public Contact team. There are no cameras in the break room or the area leading to the break room. The notebook was used to write down identifying information for the call, not as a production log.

)8/15/14:
The investigation has been completed and a spreadsheet has been created to show the number of affected individuals and includes their contact nformation.

)8/26/14:
The Incident Resolution Service Team is waiting for the PO to determine the total number of Veterans affected.

)9/09/14:
The analysis has been completed by the facility staff. All 269 Veterans whose information was in the notebook will be sent Credit Protection Service CPS) offers.

**)BCT Decision Date:** 08/19/2014

**)BCT**

he DBCT concurred that credit protection is appropriate.

| | |
|---|---|
| **Security Privacy Ticket Number:** | PSETS0000107764 |
| **Incident Type:** | Mishandled/ Misused Physical or Verbal Information |
| **Organization:** | VHA VHACO 119D<br>Pharmacy Group<br>NATIONAL CMOP 770<br>Leavenworth, KS |
| **Date Opened:** | 8/12/2014 |
| **Date Closed:** | 8/18/2014 |
| **Date of Initial DBCT Review:** | N/A |
| **VA-NSOC Incident Number:** | VANSOC0609536 |
| **Date US-CERT Notified:** | 8/12/2014 |
| **US-CERT Case Number:** | INC000000390885 |
| **US-CERT Category:** | Category 6 - Investigation |
| **No. of Credit Monitoring:** | |
| **No. of Loss Notifications:** | 1 |
| **DBCT Category:** | CMOP Mismailed |

**Incident Summary**

Patient A received a prescription intended for Patient B. Patient B's name and type of medication were compromised. Patient A reported the incident to the medical center 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. The CMOP employee(s) will be counseled and retrained in proper packing procedures.

**Incident Update**

08/12/14:
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**

The CMOP employee was counseled and retrained in proper packing procedures on 8/12/14. A patient notification letter was mailed on 8/12/14.

**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 9 Mis-Mailed CMOP incidents out of 6,307,465 total packages (9,221,405 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.

| | |
|---|---|
| **ecurity Privacy Ticket Number:** | PSETS0000107952 |
| **ncident Type:** | Mishandled/ Misused Electronic Information |
| **Organization:** | VISN 08<br>Gainesville, FL |
| **Date Opened:** | 8/15/2014 |
| **Date Closed:** | 8/29/2014 |
| **Date of Initial DBCT Review:** | N/A |
| **/A-NSOC Incident Number:** | VANSOC0609724 |
| **Date US-CERT Notified:** | 8/15/2014 |
| **JS-CERT Case Number:** | INC000000391953 |
| **JS-CERT Category:** | Category 6 - Investigation |
| **No. of Credit Monitoring:** | 2 |
| **No. of Loss Notifications:** | |
| **DBCT Category:** | Mishandling |

**ncident Summary**

he Release of Information (ROI) clerk created and provided a Veteran a CD with her medical records but inadvertently included two other Veteran's nedical records on the same CD. The Veteran returned the CD to VA and was provided a CD with only her records.

**ncident Update**

8/15/14:
he Incident Resolution Service Team has determined that both Veterans whose information was disclosed will be sent letters offering credit protection ervices.

**Resolution**

The employee responsible for the incident has re-taken VA Privacy and Information Security Awareness and Rules of Behavior training. The employee was counseled on the importance of double checking all information before providing it to patients or third parties. The employee's supervisor suggested that once a CD is created, she remove it from the computer, then replace it, and check to verify there is only one patient's information on it.

**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 114 Mis-Handling incidents this reporting period. Because of repetition, the other 113 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.

| | |
|---|---|
| **ecurity Privacy Ticket Number:** | PSETS0000108281 |
| **ncident Type:** | Mishandled/ Misused Physical or Verbal Information |
| **Organization:** | VISN 20<br>Portland, OR |
| **Date Opened:** | 8/22/2014 |
| **Date Closed:** | |
| **Date of Initial DBCT Review:** | 8/26/2014 |
| **/A-NSOC Incident Number:** | VANSOC0610043 |
| **Date US-CERT Notified:** | 8/22/2014 |
| **JS-CERT Case Number:** | INC000000393892 |
| **JS-CERT Category:** | Category 6 - Investigation |
| **No. of Credit Monitoring:** | 1686 |
| **No. of Loss Notifications:** | 54 |
| **DBCT Category:** | Mishandling |

**ncident Summary**

A VA medical assistant took two provider panel lists home in March, 2014 to work on them over a weekend. It is estimated that approximately 1500 Veterans are included on the list. The facility Privacy Officer is attempting to get an accurate list at this time. In August, 2014, the medical assistant's husband had found the list and told the nurse he is going to use it to have her fired. It was not in VA control at the time of the original incident report. The list contains the Veterans' names, Social Security numbers, VA provider names, and eligibility codes.

**ncident Update**

)8/22/14:
/A Police and the Director's office have been made aware of the situation. The Privacy Officer will update as the investigation continues.

)8/25/14:
he documents have been recovered. They are copies of originals printed in the clinic on 11/7/13. The facility believes that all pages of the documents ave been turned in. A total of 1740 Veterans' information is on the lists. The report contains the full SSNs, eligibility codes, last appointment dates, nd the first ten letters of the name (with the format being last name, first name up to ten letters total). The husband turned the documents in voluntarily o VA Police and he signed a statement saying that he found the documents in the garage of their residence on 8/18/14 and did not make copies of them or how them to anyone else. The Data Breach Core Team will review this incident during the 8/26/14 meeting.

)8/26/14:
he DBCT has determined that this is a data breach. Credit protection services will offered to all Veterans involved. If any of the Veterans are eceased, their next of kin will be sent notification letters. This is a HITECH Act breach and the required press release will be made within the 60 day vindow required.

)9/03/14:
he facility has found that 54 of the Veterans are deceased and their next of kin will be sent notification letters. At this point 1686 Veterans will be sent redit protection services letters.

)9/09/14:
he facility plans to have the draft letters and press release to the Incident Resolution Service Director for review by 09/26/14.

**)BCT Decision Date:** 08/26/2014

**)BCT**

he DBCT has determined that this is a data breach based on the fact that the husband had access to Veteran data and the employee took the documents ff site without supervisory approval.

| | |
|---|---|
| **Security Privacy Ticket Number:** | PSETS0000108349 |
| **Incident Type:** | Mishandled/ Misused Physical or Verbal Information |
| **Organization:** | VISN 12<br>Milwaukee, WI |
| **Date Opened:** | 8/25/2014 |
| **Date Closed:** | 9/8/2014 |
| **Date of Initial DBCT Review:** | N/A |
| **VA-NSOC Incident Number:** | VANSOC0610114 |
| **Date US-CERT Notified:** | 8/25/2014 |
| **US-CERT Case Number:** | INC000000394520 |
| **US-CERT Category:** | Category 6 - Investigation |
| **No. of Credit Monitoring:** | |
| **No. of Loss Notifications:** | 210 |
| **DBCT Category:** | Mismailed |

**Incident Summary**

Several Veterans returned letters postmarked on 08/22/14 that contained a generic letter outlining the new facility procedures regarding opioid treatment. The letters contained the Veterans' correct street address, but were paired with different names of other Veterans. It is unknown at this time how many Veterans received correspondence meant for other named Veterans.

**Incident Update**

)8/26/14:
The letter is a form letter that describes the new facility processes that surround a Veteran having an opioid prescription. The letter itself contains no identifiable information. However, each incorrect recipient is getting another Veteran's name on the envelope, paired with the fact that said Veteran is taking an opioid of some sort.

The Privacy Officer (PO) spoke with the person responsible. She was working with a spreadsheet of about 2400 Veterans, and it looks like an unknown quantity of them shifted. This occurred because of a mistake made with the mail merge in Word. She is going to try to replicate the results with the names and addresses. Each of the Veterans should have received this form letter, regardless of whose name was on the envelope.

)9/01/14:
After the investigation was completed, it was determined that a total of 210 Veterans were impacted. They were able to duplicate the error. Each Veteran received a copy of the letter enclosed in an envelope with a label on the form that contained their address, but another Veteran's full name from the list.

The Incident Resolution Service Team determined that each of the 210 Veterans will receive a HIPAA letter of notification.

**Resolution**

The error was able to be duplicated by Pharmacy staff to determine the number of affected patients. Letters were sent to the 210 individuals who received the incorrect letters asking them to be returned with included postage-paid self-addressed envelopes. The letters instruct the patients to return the envelope to the Privacy Office. The Pharmacy Division Manager has been alerted of the issue and will assure correct data management in the future.

**DBCT Decision Date:** N/A

**DBCT**

No DBCT decision needed. This is informational due to the number of Veterans affected.

| | |
|---|---|
| **Security Privacy Ticket Number:** | PSETS0000108501 |
| **Incident Type:** | Mishandled/ Misused Physical or Verbal Information |
| **Organization:** | VISN 08<br>West Palm Beach, FL |
| **Date Opened:** | 8/28/2014 |
| **Date Closed:** | 9/12/2014 |
| **Date of Initial DBCT Review:** | N/A |
| **VA-NSOC Incident Number:** | VANSOC0610265 |
| **Date US-CERT Notified:** | 8/28/2014 |
| **US-CERT Case Number:** | INC000000395534 |
| **US-CERT Category:** | Category 1 - Unauthorized Access |
| **No. of Credit Monitoring:** | |
| **No. of Loss Notifications:** | 52 |
| **DBCT Category:** | Mishandling |

**Incident Summary**

A Motor Vehicle Operator informed his Supervisor that he left the clipboard from his vehicle, his daily work schedule and his VA issued cell phone on the roof of the government minivan he was driving. The employee thinks he drove away with these items on top of the vehicle. He tried to reverse his route but could not find any of the missing items.

**Incident Update**

09/02/14:
The clipboard from the vehicle contained the work schedule for the day and the Special Mode Appointment List for 08/28/14. The appointment list contains 52 Veterans' full names, last four numbers of their SSN, full address, and contact phone number. The Incident Resolution Service team determined that the 52 Veterans will receive a HIPAA letter of notification.

**Resolution**

The VA Police have been notified and a VA Police report is being completed for the missing VA cell phone. A copy of the missing document (Special Mode Transportation List) was provided to the Privacy Officer by the Motor Vehicle Operator Supervisor. Letters were mailed to the 52 Veteran's involved on 09/10/2014. Copy of redacted letter uploaded. Requesting this ticket closed.

**DBCT Decision Date:** N/A

**DBCT**

No DBCT decision needed. This is informational due to the number of Veterans affected.

| | |
|---|---|
| **Security Privacy Ticket Number:** | PSETS0000108521 |
| **Incident Type:** | Missing/Stolen Equipment |
| **Organization:** | VISN 21<br>Palo Alto, CA |
| **Date Opened:** | 8/28/2014 |
| **Date Closed:** | 9/5/2014 |
| **Date of Initial DBCT Review:** | N/A |
| **VA-NSOC Incident Number:** | VANSOC0610289 |
| **Date US-CERT Notified:** | 8/28/2014 |
| **US-CERT Case Number:** | INC000000395552 |
| **US-CERT Category:** | Category 1 - Unauthorized Access |
| **No. of Credit Monitoring:** | |
| **No. of Loss Notifications:** | |
| **DBCT Category:** | IT Equipment Inventory |

**ncident Summary**

The facility Chief Information Officer (CIO) has informed the Information Security Officers (ISOs) that following a wall to wall inventory, the most ecent Report of Survey included 120 PCs, 18 phones, and 13 laptops that were determined to be lost, missing or stolen during the survey period 013-2014. This IT asset inventory control and accountability issue is a known material weakness affecting many VHA facilities and is currently the ubject of a local ongoing review involving Logistics Services and Office of Information and Technology (OI&T) personnel that is seeking ways to mprove the tracking and accountability of IT assets and to prevent loss. Palo Alto ISOs are now working with local Palo Alto VA Police, Logistics Management Services, and OI&T to review the report of survey process and to ensure that going forward, the ISOs will be included in the distribution of hese Reports of Survey so that they can create a rollup security incident ticket and thereby keep Field Security Service leadership informed of this mportant issue.

n anticipation of NSOC inquiries into this matter, the following additional information is included:

According to the Palo Alto VA Campus Chief of Police, serial numbers and descriptions of these assets are uploaded to a National Police Registry in ase they are recovered.

There is no single cause for why IT assets end up on the Report of Survey. Some suggestions are that these items were turned in or disposed of vithout proper accounting, they may have been misplaced and could still be located, and even that theft from storage, warehouse receiving docks, and vork areas could have occurred.

Logistics and OI&T are unable to determine if hard drives were removed prior to these assets being reported missing.

According to the Palo Alto OI&T Customer Support Branch, all PCs and laptops that are placed in use are routinely encrypted according to VA onfiguration guidelines.

Network share drives are created for all users and their profiles are associated with these drives and users are instructed to save documents or other iles on the network share drive, and not the local hard drive.

PCs and laptops on the Report of Survey are blocked from accessing the VA's Network. Phone accounts have been disabled.

The planned future implementation of a radio frequency identification (RFID) tag inventory tracking system is expected to greatly improve ccountability.

**ncident Update**

9/01/14:
All PCs and laptops that are currently placed in service are routinely encrypted according to VA configuration guidelines.

**Resolution**

/A Palo ISO Office has uploaded a spreadsheet containing the descriptions, serial numbers, model/model, VA inventory number, asset values, and last nown location of IT items reported lost or stolen. At present, there is no additional information available.

**DBCT Decision Date:** N/A

**DBCT**

No DBCT decision is required. This is informational for IT Equipment Inventory incidents and is the representative ticket. There were a total of 9 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 8 is not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

| | |
|---|---|
| Total number of Internal Un-encrypted E-mail Incidents | 92 |
| Total number of Mis-Handling Incidents | 114 |
| Total number of Mis-Mailed Incidents | 138 |
| Total number of Mis-Mailed CMOP Incidents | 9 |
| Total number of IT Equipment Inventory Incidents | 9 |
| Total number of Missing/Stolen PC Incidents | 1 (1 encrypted) |
| Total number of Missing/Stolen Laptop Incidents | 9 (9 encrypted) |
| Total number of Lost BlackBerry Incidents | 17 |
| Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents | 3 |