DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Risk Management and Incident Response
Incident Resolution Team

**Monthly Report to Congress of Data Incidents**
**Jan 31 - Feb 27, 2011**

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| SPE000000057655 | Mishandled/ Misused Physical or Verbal Information | Corporate Data Center Operations (CDCO) Hines, IL | 1/31/2011 | 2/1/2011 | Medium |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| | 1/31/2011 | INC000000132996 | N/A | N/A | N/A | 1 | |

**Incident Summary**

Veteran A received Veteran B's claim information in the same envelope as his own.

**Incident Update**

01/31/11:
The information disclosed included Veteran B's name, date of birth, and full social security number. Veteran B will be offered credit protection services.

**NOTE: There were a total of 108 Mis-Mailed incidents this reporting period. Because of repetition, the other 107 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.**

**Resolution**

The credit protection letter was mailed on 02/01/11.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| SPE000000057672 | Mishandled/ Misused Physical or Verbal Information | VISN 08<br>West Palm Beach, FL | 1/31/2011 | 2/11/2011 | Medium |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| | 1/31/2011 | INC000000133045 | N/A | N/A | N/A | 1 | |

**Incident Summary**

A VA employee found patient information from the Pyxis medication dispensing machine on the floor within the facility.

**Incident Update**

02/01/11:
This involved one patient, and included his social security number and date of birth. It was generated and evidently misplaced by a member of the Anesthesiology Staff. It was found in a public area. The patient will be offered credit protection services.

**NOTE: There were a total of 79 Mis-Handling incidents this reporting period. Because of repetition, the other 78 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.**

**Resolution**

The Anesthesiology Service was contacted to review policies and procedures with Service staff. Education will be provided to the Service by the Privacy Officer regarding the safe handling/disposal of information containing personally identifiable information (PII) & protected health information (PHI).

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| SPE000000057697 | Mishandled/ Misused Physical or Verbal Information | VHA CMOP Hines, IL | 2/1/2011 | 3/1/2011 | Medium |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| | 2/1/2011 | INC000000133169 | N/A | N/A | N/A | | 1 |

**Incident Summary**

Patient A received a prescription document from Medline Industries that was intended for Patient B along with his own prescription and documents. Patient B's name and type of medical supply was compromised. Patient A reported the incident to the medical center and the medical center is retrieving the document. Great Lakes Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a Medline packing error.

**Incident Update**

02/01/11:
Patient B will be sent a letter of notification.

**NOTE: There were a total of 12 Mis-Mailed CMOP incidents out of 5,898,222 total packages (9,111,763 total prescriptions) mailed out for this reporting period. Because of repetition, the other 11 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.**

**Resolution**

The packing error has been reported to Medline for investigation and corrective action.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| SPE000000057709 | Missing/Stolen Material (Non-Equipment) | VISN 09<br>Louisville, KY | 2/1/2011 | | Medium |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| | 2/1/2011 | INC000000133194 | N/A | N/A | N/A | | |

**Incident Summary**

A newly purchased laptop was delivered to the VA Warehouse loading dock, signed for by the Warehouse staff and then disappeared. The VA Warehouse staff is unable to account for laptop. No information was stored on the device as it was never taken out of the box.

**Incident Update**

02/02/11:
Information Technology Staff spoke with the VA Police and are going to complete a Report of Survey for this item but they want to do further research on the tracking number to make absolutely certain that they had the laptop shipped to them. The Warehouse workers and the IT staff inventory technician have been interviewed by the Information Security Officer (ISO) and they are continuing to investigate but are proceeding as if the item is unrecoverable.

02/07/11:
The Chief Information Officer (CIO) reports that it was received by VA, and there has been a documentation issue. The CIO believes it has been shipped back to the company, but he does not have the proper documentation to show that. The laptop was never imaged and contains no VA data.

02/18/11:
The ISO cannot confirm that this was shipped back to the company. The facility is proceeding as though this is lost equipment by preparing the Report of Survey.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| SPE000000057712 | Missing/Stolen Material (Non-Equipment) | VISN 11<br>Detroit, MI | 2/1/2011 | 3/1/2011 | Low |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| | 2/1/2011 | INC000000133208 | N/A | N/A | N/A | | |

**Incident Summary**

During inventory, a laptop listed on the EIL (equipment inventory list) was not found. A search was conducted for the laptop, but it still came up missing. The laptop was intended to be used for I-Med consents in Radiology, but since the wireless connection was not very strong, and the laptop could not connect to the VA network, it was rarely used. The laptop was not encrypted.

**Incident Update**

02/01/11:
After interviewing the staff, the Information Security Officer (ISO) determined that there was no personally identifiable information (PII) or protected health information (PHI) stored on the laptop. It was seldom used. A Report of Survey will be completed for this item.

**NOTE: There were a total of 4 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 3 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.**

**Resolution**

During the Report of Survey investigation, it was determined that the laptop was lost. It was a non-functional laptop and did not store any PII.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| SPE000000057740 | Missing/Stolen Material (Non-Equipment) | VISN 20<br>Portland, OR | 2/1/2011 | 3/2/2011 | Medium |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| | 2/1/2011 | INC000000133311 | N/A | N/A | N/A | | |

**Incident Summary**

A box of 50 to 75 Veterans Identification Cards (VIC) was discovered missing from the Enrollment Office. These cards were being held for homeless Veterans or Veterans whose cards were returned to the facility due to bad mailing addresses. The information lost includes the Veterans' full names and photograph, plus the full social security number, and date of birth contained in the barcode on the ID. Many of the cards were still in the envelopes that they had been originally mailed in so some Veterans' previous mailing address may have been disclosed as well. There is not a log of which cards were in the box so the identities of the Veterans involved are unknown. The cards were kept in an unlocked middle drawer behind the receptionist desk. The office is always locked after hours and on weekends. A complete search of the office has been made and VA Police have been notified.

**Incident Update**

02/07/11:
The Privacy Officer (PO) explained the only way to attempt to produce a list would be to request a list of recently printed cards from Austin. He would then sort out the homeless and incarcerated Veterans whose mailing address would have been our facility address. Without a way to contact these Veterans, the PO cannot tell which of them had actually picked up their new card. The remainder of the list would then likely need to be called to find out who had not received their new card in the mail.

02/23/11:
When a new card is needed, the local VA Enrollment Office takes a new picture and enters the information into the VIC system that interfaces with VistA at the local facility and automatically transmits the necessary data to the national vendor who prints and mails the cards. The office supervisor discovered that he still has the ability to run a report of all cards requested during a date range. The PO will ask him for a report to determine how many cards were printed.

02/24/11:
Since these are homeless Veterans or Veterans who recently moved, VA cannot mail notification or provide credit protection services by mail. A notice will be posted throughout the medical center and on the VA website regarding this incident. Veterans can check to see if their VIC card was among the ones that went missing and if so, instructions will be provided on how to obtain credit protection services.

**Resolution**

Staff will maintain an electronic list of all cards printed and picked up from this point forward. The box of cards is now kept in a locked drawer in a locked office.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| SPE000000057803 | Missing/Stolen Material (Non-Equipment) | VISN 22<br>Los Angeles, CA | 2/2/2011 | | Medium |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| | 2/2/2011 | INC000000133434 | N/A | N/A | N/A | 0 | 25 |

**Incident Summary**

On 02/02/11, an employee reported that a laptop connected to an electromyography (EMG) device at the West LA campus was stolen. The laptop was not encrypted because it was connected to a medical device. The laptop was last seen on 01/27/11. The laptop contained an undetermined number of patients' last name and last 4 of the SSN. The laptop was not connected to the Network and has been non-functional for months.

**Incident Update**

02/02/11:
There are no cameras in the area. The laptop was secured to the top of the EMG unit. It was stored in an exam room that is located within the Physical Medicine & Rehabilitation Outpatient Clinic. The outer doors of the clinic were locked. The exam room where the laptop was located also locks, but the Information Security Officer (ISO) cannot confirm if the door was locked during the period of time that the laptop was taken. The Report of Survey was submitted to the ISO.

02/04/11
The information that could be on the laptop is the last name and last 4 of SSN which would be associated with wave forms with numerical data. There is no clinical history, assessment, interpretation or treatment plan information. There may be up to 20 VA patients' information on the laptop. The clinicians will provide a list of the days they used the machine and compare that to VistA appointment records to get an exact count. Also, Information/results are manually documented in Computerized Patient Record System (CPRS) by the house staff/attending physician.

02/08/11:
Through process of elimination, the Privacy Officer identified approximately 125 potential patients, of which 20-25 of these patients may have information (last name and last four of social security number) stored on this laptop. Therefore, 25 Patients will receive a notification letter.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| SPE000000058013 | Missing/Stolen Equipment | VISN 16<br>Houston, TX | 2/7/2011 | 3/2/2011 | Low |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| | 2/7/2011 | INC000000134015 | N/A | N/A | N/A | | |

**Incident Summary**

On 02/07/11, a VA employee reported that 2 PCs were missing (possibly stolen) to VA Police. The file clerk stated that the PCs may have been taken between 02/04/11 and 02/06/11, when the department was closed. The file clerk has also notified Information Management Services (IMS) to ensure that the PCs were not taken for routine PC maintenance or replacement of inventory. The Chief Information Officer (CIO), Chief of Police, Information Security Officer (ISO) and Executive Administrator were notified. The VA employee stated that no patient data was on the hard drive and the PCs were used as dumb terminals to print out appointments for patients from Computerized Patient Record System (CPRS) and to access VistA.

**Incident Update**

02/08/11:
The clinical supervisor informed the ISO that only 1 PC is missing. The ISO will obtain the police report number from VA Police Officer.

02/28/11:
The ISO has received a copy of the police report. The ISO and IT Department confirmed that no sensitive data was lost or missing due to fact that the PC was used as an access point for the CPRS, and not for storing data.

**Resolution**

The ISO has confirmed with VA Police that the missing PC was not recovered during the initial investigation. However, the VA Police will transfer the case to the detective for further review.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| SPE000000058067 | Mishandled/ Misused Physical or Verbal Information | VISN 04<br>Clarksburg, WV | 2/8/2011 | | Medium |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| | 2/8/2011 | INC000000134191 | N/A | N/A | N/A | 1629 | |

**Incident Summary**

A VA employee planning to use a government vehicle found a packet of information containing patient names, SSNs, and appointment dates. The preliminary investigation determined that the packet had been left in the vehicle by another employee on 10/26/10.

**Incident Update**

03/04/11:

The Associate Director (AD) and Privacy Officer investigated this incident and found that on 10/26/10, the supervisor utilized the vehicle to provide training. Apparently this packet of information fell out of her folder between the seats or under the seat. It was clipped together along with being stapled, so there is no reason to believe any pages are missing.

Between 10/27/10 and 11/16/10, there were 14 government employees who utilized this vehicle. None of them recall seeing any papers in this vehicle, which indicates they had indeed slid between the seat and console or under the seat and out of sight. These were all government employees, and would not have had any civilians or family members in the vehicle with them.

Between 11/16/10 and 01/31/11, the vehicle was locked and parked in facility parking lot after being involved in a collision with a deer on 11/16/10. On 01/03/11, the vehicle was taken to a body shop to have the damaged fender and headlight replaced. The VA employee who took the vehicle over to the body shop and picked it up on 02/02/11 did not see any paperwork lying in the car, again indicating that this sensitive information was not in visible sight of anyone getting into or out of the car.

Between 02/02/11and 02/08/11, there were 2 employees who drove this vehicle after the repairs had been made and prior to the information being discovered. Again, no one other than VA employees would have been in or driven this vehicle during that time.

The AD believes that on late 02/07/11 or early 02/08/11, the car was cleaned and detailed by VA staff. The AD has not yet identified which staff member, but believes that while vacuuming the car and cleaning it that the staff member found this information between the seats or under the seat and set it on the front passenger seat to be found. On 02/08/11, the employee planning to use this vehicle that day saw the information and reported it. The supervisor who provided the CBOC training was reeducated on securing sensitive personal information. The 1629 patients will receive a letter offering credit protection services and will be reported to HHS under the HITECH Act.

| | |
|---|---|
| Total number of lost Blackberry incidents | 30 |
| Total number of internal un-encrypted e-mail incidents | 84 |
| Total number of Mis-Handling Incidents | 79 |
| Total number of Mis-Mailed Incidents | 108 |
| Total number of Mis-Mailed CMOP Incidents | 12 |
| Total number of IT Equipment Inventory Incidents | 4 |
| Total number of Missing/Stolen PC Incidents | 3 |
| Total number of Missing/Stolen Laptop Incidents | 11 (4 encrypted, 3 new) |