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.

November 5 - December 2, 2012

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000081970	Mishandled/ Misused Physical or Verbal Information	VISN 09 Lexington, KY	11/5/2012	11/7/2012	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
VANSOC0582543	11/5/2012	INC000000245255	N/A	N/A	N/A	1	

Incident Summary

Veteran A received Veteran B's medication in the mail. The protected health information (PHI) that was compromised included Veteran B's full name, last four digits of the SSN and date of birth. The Information was outside of VA control for less than 72 hours and involved one Veteran.

Incident Update

11/05/12:
Veteran B will be sent a letter offering credit protection services.

NOTE: There were a total of 82 Mis-Mailed incidents this reporting period. Because of repetition, the other 81 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

Staff was reminded to be more careful when handling PHI.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000082045	Missing/Stolen Equipment	VISN 06 Fayetteville, NC	11/6/2012		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
VANSOC0582620	11/6/2012	INC000000245577	N/A	N/A	N/A		

Incident Summary

During the annual inventory audit, several items were reported missing and/or unaccounted for. The Facility Chief Information Officer (CIO) reported this to the Information Security Officer (ISO).

Incident Update

11/13/12:
A Report of Survey (RoS) Team is investigating this inventory. When the team's investigation is completed, they will provide their findings and recommendations to Executive Leadership for review and signature/approval. When this is completed an electronic copy will be provided to the ISO for uploading to this ticket. This will take approximately 10-14 days for this process to be completed.

12/04/12:
The ISO sent a follow-up email to the Logistics Service requesting the status of RoS and to ask whether the RoS had been signed. The ISO requested that an electronic copy be provided to upload to the ticket.

12/05/12:
The ISO received a copy of the RoS however the RoS is still ongoing. So far there are 116 items that are missing or unaccounted for. During the course of the inventory, they found that several items were mislabeled, making them difficult to track.

NOTE: There were a total of 3 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.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000082086	Mishandled/ Misused Physical or Verbal Information	VISN 07 Charleston, SC	11/7/2012	12/5/2012	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
VANSOC0582661	11/7/2012	INC000000245787	N/A	N/A	N/A	1	

Incident Summary

The Privacy Officer (PO) received an email at 9:51 AM this morning from the Compliance Officer stating that she found documents on a table by the elevator on the second floor of the VAMC at 4:15 PM on 11/02/12. The PO noted that that Veteran had a procedure done that day at about 11:00 AM and was discharged at approximately 2:00 PM. The PO is going to retrieve the documents from the Compliance Officer and go to Ambulatory Surgical Department for additional information.

Incident Update

11/13/12:
The PO spoke with the Veteran whose paperwork was left in second floor elevator lobby. The Veteran and his spouse said they did not receive the paperwork. They stated they only received paperwork informing the Veteran of his next appointment. The Veteran stated that he left close to 2:00 PM so approximately two and a half hours passed before our Compliance Officer found the documents. However, his procedure was done on the fourth floor and recovery is on the third floor so the PO has no idea how it ended up on the second floor of the VAMC. Therefore, Veteran A will receive a letter offering credit protection services.

NOTE: There were a total of 95 Mis-Handling incidents this reporting period. Because of repetition, the other 94 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 PO could not prove who left documents in second floor elevator lobby. The Veteran received procedure on the fourth floor and transferred to third floor for observation. His wife was given paperwork pertaining to his upcoming visits but stated that was all she was given. The Veteran was discharged about 2:00 PM which he confirms. The Veteran and his wife never went to the second floor but headed straight home. A Nurse in Ambulatory Surgery stated she always gives the Post Upper Endoscopy Instructions to the patient when they are discharged. Since the spouse had some paperwork, the PO believes all of the documents would have been given at the same time. The PO cannot determine after talking with staff, Veteran, and family member, who left the documents in the second floor elevator lobby.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000082097	Missing/Stolen Equipment	VISN 11 Detroit, MI	11/7/2012		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
VANSOC0582674	11/7/2012	INC000000245811	N/A	N/A	N/A		

Incident Summary

A desktop PC is missing from the Radiology conference room. The last time the PC was seen was on 02/02/12 during an inventory. The Radiology conference room in the Radiology suite is sometimes locked during the day but the secretary and the Administrative Officer (AO) check to make sure the room is locked every night. There may be a possibility that the computer was moved. The Information Security Officer (ISO) is waiting on the Police Report.

Incident Update

11/27/12:
There is no new information on this missing computer. The VA Police report was filed.

Resolution

The VA Police will put the report in abeyance and if the computer comes up a flag will show up and notify the Police of the missing computer.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000082195	Mishandled/ Misused Physical or Verbal Information	VISN 08 San Juan, PR	11/9/2012		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
VANSOC0582778	11/9/2012	INC000000246256	N/A	N/A	N/A	116	47

Incident Summary

While performing Environment of Care (EOC) rounds in the Surgical ICU area, a member of the team found a box full with documents pertaining to Veterans and employees under a sink. The box was left open and unattended in a lounge area shared by employees of the Surgical ICU and Dental Service. The documents were from 1999 to 2004.

Incident Update

11/20/12:
There is no restriction of the area. It is an open lounge.

In total there are 163 cases divided as follows:
1) 75 Veterans with full name and full SSN
2) 41 Employees with full name and full SSN
3) 47 Employees with full name and partial SSN

11/27/12:
The DBCT decided that the 75 Veterans with full name and full SSN will get a letter offering credit protection services, the 41 employees with name and full SSN will get a letter offering credit protection services and the 47 employees with name and partial SSN will get general notification letter.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000082698	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Leavenworth, KS	11/20/2012	11/21/2012	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
VANSOC0583286	11/20/2012	2012-USCERTv3437IEN	N/A	N/A	N/A		1

Incident Summary

Patient A received a prescription intended for Patient B. Patient B's name, address, and type of medication were compromised. Patient A reported the incident to the medical center and a replacement has been requested for Patient B. Leavenworth 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

11/20/12:
Patient B will be sent a notification letter due to Protected Health Information being disclosed.

NOTE: There were a total of 3 Mis-Mailed CMOP incidents out of 6,060,063 total packages (8,999,862 total prescriptions) mailed out for this reporting period. Because of repetition, the other 2 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 CMOP employee(s) will be counseled and retrained in proper packing procedures.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000082734	Mishandled/ Misused Physical or Verbal Information	VBA Salt Lake City, UT	11/20/2012		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
VANSOC0583318	11/20/2012	INC000000248100	N/A	No	N/A	64	146

Incident Summary

While reviewing another incident, the Fiduciary Hub identified that a batch of letters that was sent in the South East Region in October 2012 contained the name and SSN or claim number of other Veterans. Specifically they reported "The batch of letters sent in the South East Region in October consisted of 210 pre-contact letters. The printer settings had been changed on the printer and forced double sided prints. This caused each second letter to begin on the back page of the prior letter for letters of the South East Region. There were 210 letters printed and mailed in the South East Region.

Incident Update

11/26/12:
Because the facility is unable to determine which of the 210 received the information of the others, the facility would like to send letters to all 210. The 210 Veterans will receive letters offering credit protection services due to full name and full SSN being disclosed.

11/27/12:
After further investigation, it was determined that there were only 64 letters that had the full SSN printed on them. The remaining 146 letters had the VA claim number. All of the letters had the name and address on them. Therefore, 64 Veterans will receive letters offering credit protection services. The other 146 Veterans will receive general notification letters.

Resolution

The appropriate corrective action has occurred.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000082999	Mishandled/ Misused Electronic Information	VISN 08 Miami, FL	11/30/2012	12/4/2012	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
VANSOC0583584	11/30/2012	INC000000249700	N/A	N/A	N/A		81

Incident Summary

An OIG Investigation found the inappropriate disclosures of patient information to third parties (friends of an employee) and the emailing of sensitive information, including personally identifiable information (PII) and protected health information (PHI), to the employee's personal email account. There were at least 55 patients affected. The employee was a home based provider. Further details are pending.

Incident Update

11/30/12:
Eighty-one names were emailed to a private email account in an attachment. Each contained the first name, last name, address, telephone number, and assessment date. Of the 81 discovered, 70 contained the last four digits of the SSN, 9 contained last three digits of the SSN, 1 contained last two digits of the SSN, and 1 contained last one digit of the SSN. There was one email that did contain medical information and date of birth. Therefore, 81 patients will receive notification letter and on patient will receive a letter offering credit protection services.

12/03/12:
The one Veteran whose SSN was exposed is now deceased therefore a next of kin (NOK) notification letter will be sent.

Resolution

The provider's access to patient records has been terminated. Notification letters to patients and NOK have been sent.

Total number of Internal Un-encrypted E-mail Incidents	75
Total number of Mis-Handling Incidents	95
Total number of Mis-Mailed Incidents	82
Total number of Mis-Mailed CMOP Incidents	3
Total number of IT Equipment Inventory Incidents	3
Total number of Missing/Stolen PC Incidents	3
Total number of Missing/Stolen Laptop Incidents	13 (13 encrypted)
Total number of Lost BlackBerry Incidents	19
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	3