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
October 3 - 30, 2011

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000067434	Mishandled/ Misused Physical or Verbal Information	VISN 01 West Haven, CT	10/4/2011	10/14/2011	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
	N/A	N/A	N/A	N/A	N/A	1	

Incident Summary

Patient A called the Patient Advocate to report that he received lab orders belonging to Patient B. The lab orders included Patient B's name, full SSN and medical information.

Incident Update

10/11/11:
Patient B will be sent a letter offering credit protection services due to full name and full SSN being disclosed.

NOTE: There were a total of 81 Mis-Mailed incidents this reporting period. Because of repetition, the other 80 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 staff was provided educational training by their supervisor. The information has been returned in its entirety.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000067493	Mishandled/ Misused Physical or Verbal Information	VISN 02 Buffalo, NY	10/6/2011	10/17/2011	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
	10/6/2011	INC000000175160	N/A	N/A	N/A	9	

Incident Summary

A staff member made copies of nine wrist bands stapled together. They were used to bypass BCMA and the need for scanning the wristband on the patient. The copies fell out of the staff member's pocket on the floor in Canteen. The Information Security Officer (ISO) found the copies and handed them over to the Privacy Officer (PO).

Incident Update

10/06/11:
Nine Veterans will be sent a letter offering 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 ISO ran a report to show who had printed the wristbands. The report identified several individuals who were counseled/sanctioned. The Nursing supervisor will monitor the process going forward.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000067529	Missing/Stolen Equipment	VISN 18 Albuquerque, NM	10/7/2011	10/28/2011	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
	10/7/2011	INC000000175410	N/A	N/A	N/A		

Incident Summary

A VA employee discovered the My HealtheVet computer located in the General Medicine Clinic was missing on Saturday night 10/01/11. Information Resource Management (IRM) was contacted to see if they moved the PC and they had not. The cables, mouse and keyboard were left on the table. The monitor and CPU were missing.

Incident Update

10/11/11:
The incident is still under investigation.

10/17/11:
There are no cameras in the area and the cameras covering the entrances did not show anyone taking a computer out. The My HealtheVet PCs are locked down and do not store sensitive data on them.

10/28/11:
PC has been listed as stolen.

Resolution

Per the Police Service this PC is considered stolen. No video surveillance is available. This was a My HealtheVet kiosk machine and the PC are locked to prevent storing of information on them.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000067571	Mishandled/ Misused Physical or Verbal Information	VISN 07 Tuscaloosa, AL	10/10/2011		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
	10/10/2011	INC000000175639	N/A	N/A	N/A	210	9

Incident Summary

The Privacy Officer was notified that a Veteran from the Psychosocial Residential Rehabilitation Treatment Program (PRRTP) was in the Veterans' Cyber Cafe using a computer and discovered approximately 10-12 sheets of paper lying face down across the corner of the printer. The Veteran picked them up, noted they were lists of inpatient Veterans with full SSNs, dates of admission, diagnoses, and ages. He stated he saw his own name and knew that he needed to let someone know he had found these papers. The Veteran returned to his unit and turned in the papers in to the LPN on duty.

Incident Update

10/17/11:
Two hundred ten Veterans will be sent letters offering credit protection services due to full name and full SSN being exposed. Nine next-of-kin notifications will be sent on behalf of the nine of the affected Veterans who are deceased.

11/01/11:
The investigation by the PO is complete. The letters are in review and awaiting signature. The letters will start going out this week.

Here are several recommendations made by the PO:
*The immediate supervisor to provide a copy of the Local Privacy Policy's attachment "Clean Desk Policy" to the VA employee and to obtain a signature indicating the receipt and acknowledgement of the policy's attachment that covers safeguards and protection of all veteran sensitive information.
*Encourage not creating any paper documents if at all possible for assigning Medical Record Review (MRR).

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000067606	Mishandled/ Misused Physical or Verbal Information	VISN 02 Albany, NY	10/11/2011		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
	10/11/2011	INC000000175899	N/A	N/A	N/A		

Incident Summary

A daughter of Veteran A talked to a VA employee today. She stated that when her mother (Veteran A) was discharged she was given papers to assist in placement. Included in this paperwork was information on Veteran B. At this time, we have no idea what kind of information or Veteran B's identity. The daughter was asked to return paperwork which she stated she would. She did also mention calling her lawyer who told her to use this as leverage with placement of her mother.

Incident Update

10/17/11:
The Veteran A's daughter is returning the paperwork via mail. The paperwork has not been received by the facility as of 10/17/11. After the paperwork arrives at the facility the PO will be able to determine what information about Veteran B was disclosed.

10/31/11:
The facility has still not received the paperwork. The Social Worker who has been in contact with the daughter has been unsuccessful in getting back in contact with the daughter to determine if/when the daughter will be sending the paperwork back to the facility.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000067613	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Hines, IL	10/11/2011		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
	10/11/2011	INC000000175929	N/A	N/A	N/A		3

Incident Summary

Patient A received multiple prescriptions intended for three other patients. The other patients' names and types of medication were compromised. Patient A reported the incident to the medical center and returned the prescriptions in question. Great Lakes Consolidated Mail Outpatient Pharmacy (CMOP) provided replacement prescriptions for the other three patients. CMOP investigation concludes that this was a CMOP packing error. The CMOP employee will be counseled and retrained in proper packing procedures.

Incident Update

10/12/11:
Three patients will be sent a notification letters due to names and medication types being compromised.

NOTE: There were a total of 7 Mis-Mailed CMOP incidents out of 6,160,969 total packages (8,987,649 total prescriptions) mailed out for this reporting period. Because of repetition, the other 6 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	Risk Category
SPE000000067646	Mishandled/ Misused Physical or Verbal Information	VISN 20 Portland, OR	10/12/2011		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
	10/12/2011	INC000000176141	N/A	N/A	N/A		63

Incident Summary

A Campus Police Officer at the affiliate University that is physically attached to the VA Medical Center found 5 folded pages containing information about current VA surgery patients. The papers were on the ground in the hallway outside a busy campus cafeteria at approximately 10:00 AM on 10/10/11. The Officer secured the documents and filed an incident report with the University's Information Security Officer (ISO). The ISO contacted the local VHA Privacy Officer (PO) about the incident and turned over the documents.

The pages contain the full names, last 4 digits of the SSN, and medical information regarding the patient's type of surgeries and medications they were on at the time. A few non-Veteran patients are included on the spreadsheets, but it appears there are approximately 60 Veterans listed.

The Privacy Officer is looking for the surgical staff who were working on the 10/10/11 holiday weekend to determine who may have lost the paperwork.

Incident Update

10/13/11:
Notification letters will be sent to 57 Veterans and 6 University patients.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000067647	Missing/Stolen Material (Non-Equipment)	VISN 07 Birmingham, AL	10/12/2011	10/24/2011	High

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
	10/12/2011	INC000000176142	N/A	N/A	N/A	377	

Incident Summary

On 10/11/11, between 5:45 PM and 6:15 PM, a log book with personally identifiable information (PII) and protected health information (PHI) was stolen from a VA physician's car. This log book contained the following information on approximately 377 patients: full name, full SSN, DOB, name of procedure, date of procedure, and follow-up required. A Police Report was filed and the Privacy Officer (PO) will obtain a copy. The list of Veterans involved has been re-created.

Incident Update

10/13/11:
The 377 Veterans will be sent a letter offering credit protection services due to full name and SSN being disclosed.

10/17/11:
The logbook was being used to track procedures performed by the provider during his fellowship. The provider carried the log book home each night and would enter the information into a system called "e-value" which is used by an affiliate hospital to track the progress of patients.

Resolution

Credit Monitoring letters were mailed to all affected Veterans or next-of-kin on 10/20/11. The physician was counseled and has re-taken the VA Privacy and Information Security Training. The Affiliate Program Director was notified of the breach. All Gasto-Intestinal (GI) residents/fellows were instructed to immediately stop entering any PII/PHI into the e-value System as of 10/13/11. The PII/PHI was removed from the e-value system for the GI training program on 10/13/11. The PO and ISO are developing a summary of privacy/security requirements to be given to all physician trainees as part of orientation to emphasize requirements. An investigation is being conducted to determine other users of e-value system (or like systems) and appropriate action to be taken (see related SOC Ticket 67757).

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000067684	Missing/Stolen Equipment	VISN 11 Detroit, MI	10/13/2011	10/17/2011	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
	10/13/2011	INC000000176421	N/A	N/A	N/A		

Incident Summary

There is a computer missing in the Mental Health area, Chemical Dependence section. OIT did not remove the PC. OIT is checking to obtain the preventive maintenance numbers of the computer. It was reported that sensitive information could be on the computer. A Police Report has been filed. Further investigation is pending by the Information Security Officer (ISO) and the Privacy Officer (PO).

Incident Update

10/14/11:
This is an unencrypted PC which was used for CPRS. There are group policies to prevent data from being stored locally, however it is still possible that some data may have been saved to the local hard drive.

Resolution

After speaking with the employee who reported the computer missing it was determine that no sensitive information was stored on the computer. The computer was used for CPRS only.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000067761	Missing/Stolen Material (Non-Equipment)	VISN 20 Seattle, WA	10/17/2011		High

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
	10/17/2011	INC000000176960	N/A	N/A	N/A	59	

Incident Summary

A proximity card and a log book containing personally identifiable information (PII) and protected health information (PHI) were stolen from a VA Puget Sound Health Care System (VAPSHCS) doctor's vehicle while he was off VA property. There was approximately 50 patients' PII/PHI involved.

Incident Update

10/18/11:
The doctor did not have authorization to take to take documents with patient’s names off campus. The Information Security Officer (ISO) and Privacy Officer (PO) are investigating to see exactly what PII/PHI was involved and if the patients can be identified.

10/25/11:
The list of names on the log book is not known, but a list of potential names based on the residents schedule has been created. The patients' names, SSNs, and medical information were in the logbook. The residents are required to keep track of procedures, and have the authority to do so, but this included clinical information. The 59 patients whose names could have potentially been in the log book will be sent letters offering credit protection services.

Resolution

VAPSHCS Privacy Office and Information Security Office have addressed the incident through the appropriate reporting mechanism. The VA Police are actively investigating. The Service Line Leadership is discussing implementation of procedural changes and training designed to reinforce privacy concerns associated with physician logs. The Chief of Staff directed the Assistant Chief of Staff (ACOS) for Education to immediately reinforce to all house staff that the recording of PII or PHI in case logs is strictly prohibited. This will also be communicated to all the Residency Program Directors at the academic affiliate. The investigation is ongoing.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000067777	Missing/Stolen Equipment	VISN 16 Little Rock, AR	10/18/2011	10/28/2011	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
	10/18/2011	INC000000177160	N/A	N/A	N/A		

Incident Summary

On 10/06/11, the Nurse Manager of the unit reported two missing workstations from the Report Room and the Chart Room to an Office of Information Technology (OIT) technician. Neither individual reported the missing devices to the Information Security Officer (ISO) or to the VA Police. The technician informed the Nurse Manager that he would inquire about the devices with other OIT staff and do some searching. He checked log files, Service Desk tickets, Active Directory, Inventory File and system administrators. The only information found was that one of the missing workstations was last logged in on 09/09/11 and inventoried on 05/04/11. The other missing workstation was last logged in on 06/05/11 and inventoried on 05/04/11.

Neither device was encrypted. The devices were used by nursing staff and other care providers to enter data into the Computerized Patient Record System (CPRS) which does not write to the hard drive. It is reasonable to believe that there would be no storage of sensitive data on either of the devices.

Resolution

As of 10/27/2011 the investigation is still ongoing but the PC's most likely will not be recovered. No data breach occurred.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000067854	Missing/Stolen Equipment	VISN 11 Indianapolis, IN	10/20/2011	10/21/2011	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
	10/20/2011	INC000000177579	N/A	N/A	N/A		

Incident Summary

During an Office of Information Technology (OIT) inventory, a Logistics Supply Technician was unable to find a desktop PC. The person who is accountable for the equipment is a VA physician and researcher and he is unable to say positively what happened to the PC. It was last inventory was in 2009. There is no documentation to support that this equipment was turned in or excessed. It contained no personally identifiable information (PII) or protected health information (PHI).

Incident Update

10/20/11:
The PC was not encrypted and is not believed to be stolen. It is believed to be an inventory documentation error. A Report of Survey was filed.

11/01/11:
The PC was listed on the Research Equipment Inventory List, but the user is a physician who provides clinical care to Nephrology patients. The PC was in his office and he used it to access VA clinical data in support of patient care via CPRS. The physician also participates in research activities, but he has a separate research lab (with PCs) where he conducts research. It is unlikely that the user was conducting research activities on this PC.

The user reported that he never saves data to his PC's hard drive. At the Indianapolis VAMC, group policy is in place that redirects all users MY DOCUMENT folders to their secure network home drive, so it is highly unlikely that a user would save data to their PCs hard drive. All users are instructed to save their data to network drives, to not only protect PII/PHI, but because the network share data is backed up daily and their PCs are not. Finally, OIT runs an application that periodically scans PC VLANs searching for data that is formatted in a way, that it may be PII (i.e. 9 digit SSNs). While the ISO cannot be 100% sure PII/PHI was not on the PC, they do have security controls in place that lessen the likelihood of that happening. The user reported that the PC was replaced last year and he remembers someone taking it away on a cart. This is why the ISO suspects that this is an inventory related issue.

NOTE: There were a total of 3 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 2 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Resolution

All employees involved were made aware of the VISN and local policy that instructs how to properly maintain an inventory. This matter has been turned over to Human Resources (HR) for further action and resolution.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000067865	Missing/Stolen Material (Non-Equipment)	VISN 04 Pittsburgh, PA	10/20/2011	11/1/2011	High

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
	10/20/2011	INC000000177657	N/A	N/A	N/A	308	

Incident Summary

The Ears, Nose and Throat (ENT) Clinic Manager reported to the VA Police and the Privacy Officer (PO) that an unlocked/unsecured file cabinet in an unsecured area had been tampered with. The file cabinet stored documents containing protected health information (PHI) had been placed in the trash.

When a clinic administrative clerk reported to work the morning of 10/20/11, she discovered that the medical pre-op packages in the file cabinet were not in the same order as they were the previous afternoon when the clerk left for the day. There were also documents from the file cabinet that were found in the trash can. The clerk reports that the file cabinet was locked and that the cubicle where the file cabinet is located does not lock. The clerk is comparing the schedule of today's patients with the documents that have been tampered with to try and determine if any of the pre-op medical packets are missing.

Incident Update

10/20/11:
It is not known if malicious intent was involved, however it is known that someone did go through the records and left them in an unorganized fashion and two of the packets of information were thrown in the trash. The clinic manager questioned staff to see who was in the area after hours and why, however all staff members denied being in the area. All documents in the room have been reviewed and there were a total of 354 Veterans who had their information compromised. Letters offering credit protection services will be sent to 354 Veterans.

10/31/11:
The total number of individual affected was 308 and not 354. The reason the documents were unsecured is that the clerk indicated that they only had 1 key to the file cabinet and wanted to make sure access to cabinet was available to staff in the event that someone needed into the cabinet and the clerk was not available. The underlying reason or excuse for lack of proper safeguarding is based on the fact that the facility is having some remodeling completed and many clinics are working in temporary work areas.

Resolution

The credit protection letters were provided to the affected individuals. The area where the incident occurred has been properly secured and improved safeguard measures are in the process of being implemented. The file cabinet was rekeyed by the locksmith and more than 1 key is now available. The door to the check in area has been scheduled to have a lock installed. Temporary use of the locked nursing office across the hall is also being used to store all documents overnight until proper safeguard measures have been implemented and determined secure by the privacy office.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000067987	Mishandled/ Misused Physical or Verbal Information	VISN 10 Dayton, OH	10/25/2011		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
	10/25/2011	INC000000178546	N/A	N/A	N/A	65	

Incident Summary

A Release of Information (ROI) staff person inadvertently released an appointment roster with 65 Veterans' information to another Veteran. The information that was disclosed included the Veterans' full names, full social security numbers and telephone numbers.

Incident Update

10/25/11:
Sixty-five (65) Veterans will be sent letters offering credit protection services due to full name, full SSN being disclosed..

Total number of Lost Blackberry Incidents	22
Total number of Internal Un-encrypted E-mail Incidents	55
Total number of Mis-Handling Incidents	79
Total number of Mis-Mailed Incidents	81
Total number of Mis-Mailed CMOP Incidents	7
Total number of IT Equipment Inventory Incidents	3
Total number of Missing/Stolen PC Incidents	6
Total number of Missing/Stolen Laptop Incidents	12 (11 encrypted)