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
August 1 - 28, 2011

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000065395	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Hines, IL	8/3/2011	8/11/2011	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
	8/3/2011	INC000000164570	N/A	N/A	N/A		1

Incident Summary

Patient A received a medical supply intended for Patient B. Patient B's name and type of supply was compromised. Patient A reported the incident to the medical center and a replacement has been sent Patient B. Great Lakes Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error. The CMOP employee was counseled and retrained in proper packing procedures.

Incident Update

08/03/11:
Patient B will be sent a notification letter.

NOTE: There were a total of 6 Mis-Mailed CMOP incidents out of 6,109,907 total packages (8,882,867 total prescriptions) mailed out for this reporting period. Because of repetition, the other 5are 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 was counseled and retrained in proper packing procedures.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000065544	Missing/Stolen Material (Non-Equipment)	VISN 03 New York, NY	8/8/2011	9/7/2011	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
	8/8/2011	INC000000165401	N/A	N/A	N/A		

Incident Summary

A glucometer (glucose meter) from the ICU was reported missing to a Nursing Supervisor on 08/05/11. The staff searched for the glucometer but could not find it. The Nursing Supervisor reported the glucometer missing on 08/08/11 to the VA Police.

Incident Update

08/15/11:
The Information Security Officer (ISO) spoke to the Acting Nurse Manager who notified the VA Police and to the server\glucose meter point of contact (POC). The POC stated that the only information on the meter is the full SSN of the patients and the blood glucose test result. It is unknown how many patients' SSNs were on the Glucometer or which patients' SSNs were on the meter. All employees have been interviewed and none recall seeing the Glucometer. The Glucometer requires the use of a PIN number to operate or to access the data.

08/16/11:
The VA Police Report and the Report of Survey were completed.

09/02/11:
The device locks after 3 unsuccessful logons. There were approximately 215 patients whose SSN and blood glucose level was stored on the device. The facility is in the process of changing how the device is accounted for. There were approximately 35-40 nurse user accounts that were on the device.

09/08/11:
Abbott confirmed that there is no way to access the data on the glucometer without a valid PIN.

Resolution

The glucometer will now be accounted for at change of shift. Laboratory and Nursing staff will establish guidance on the frequency of clearing the data from the device. The Data Breach Core Team (DBCT) reviewed this incident and determined that based on the PIN number and the lockout feature, the risk of data compromise was low and that this incident could be closed.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000065561	Mishandled/ Misused Physical or Verbal Information	VISN 04 Pittsburgh, PA	8/9/2011	8/11/2011	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
	8/9/2011	INC000000165427	N/A	N/A	N/A	1	

Incident Summary

Patient A realized that the patient wristband placed on his wrist was not his. The wristband on his wrist pertained to Patient B. The wristband contained Patient B's name and full SSN.

Patient A identified the mistake within 30 minutes and reported it to the clinic manager. The clinic manager removed the wristband and then walked the patient up to the front desk and corrected the error. The clerk indicated that she must have made a mistake and placed the incorrect wristband on the patient. It was also verified that this was the only patient affected and no other patient wristbands were incorrectly placed on any other patients.

Incident Update

08/09/11:
Patient B will be sent a letter offering credit protection services, due to full name and full SSN being exposed.

NOTE: There were a total of 81 Mis-Handling incidents this reporting period. Because of repetition, the other 80 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 employee was reeducated by the clinic supervisor regarding this type of error and to ensure proper identification of patients when putting on patient wristbands. The clinic manager will conduct a post incident training brief at the next staff meeting and will remind all staff to perform proper ID authentication and ensure patient wristbands are checked at every step during the treatment process.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000065737	Missing/Stolen Equipment	VISN 11 Detroit, MI	8/15/2011	8/16/2011	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
	8/15/2011	INC000000166546	N/A	N/A	N/A		

Incident Summary

Over the weekend, two VA personal computers (PC), the monitors and a scanner were stolen. The computers are not believed to contain any sensitive information. The computers were not encrypted. The computers were locked down at the time of theft.

Incident Update

08/16/11:
The first PC was at the information desk and the second PC was at the mental health check-in desk. Both clerks stated that they do all of her work within CPRS and do not save any sensitive data to their hard drives. A VA Police report has been filed and a Report of Survey has been completed.

09/02/11:
VA Police are still investigating this incident. There is a camera in the general area of the information desk where the first computer was taken from. This computer was rarely used and only for web access but the camera wasn't able to pan over to the area where the computer was located. Also there is not a camera near the mental health check in desk where the second computer was taken from. There was a request to have a camera installed in this area but the funding was never provided. After speaking with the employee who works at the Mental Health check in desk it was determined that the computer in the Mental Health check in area is used to access CPRS and VISTA only and no information is ever saved outside of VISTA.

Resolution

A Report of Survey and a Police Report have been completed. From the investigation it was determined that no personally identifiable information (PII) or protected health information (PHI) was stored on the computers.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000065985	Missing/Stolen Equipment	VISN 03 New York, NY	8/22/2011	9/8/2011	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
	8/22/2011	INC000000167879	N/A	N/A	N/A		

Incident Summary

The VA Police received a complaint from the Information Security Officer (ISO) that a personal computer (PC) was missing from Centralized Scheduling. The PC was there on Friday at 3:30 PM when the employee left and was missing when the employee reported to work on Monday morning at 8:00 AM. The employee locked the door when he left on Friday afternoon. The door was closed but not locked when the employees arrived at work on Monday. The Police Report is currently being generated.

Incident Update

08/24/11:
There are no cameras in the area. The PC was not encrypted and was used in the Central Intake area. The facility uses Desktop Authority to redirect data to a network drive therefore no data was stored on the PC. The VA Police report was completed.

Resolution

The remaining computers have had locks installed to prevent removal from the area.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000065990	Mishandled/ Misused Physical or Verbal Information	VBA Muskogee, OK	8/22/2011	8/24/2011	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
	8/22/2011	INC000000167888	N/A	N/A	N/A	1	

Incident Summary

Veteran A returned a letter by certified mail that was enclosed with his letter and was intended for Veteran B. Veteran B's name and full SSN was included in the letter.

Incident Update

08/22/11:
Veteran B will be sent a letter offering credit protection services.

NOTE: There were a total of 79 Mis-Mailed incidents this reporting period. Because of repetition, the other 78 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 Information Security Officer (ISO) checked the mail machine to avoid future mismailings.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000066115	Unauthorized Electronic Access	VISN 20 Spokane, WA	8/25/2011		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
	8/25/2011	INC000000168523	N/A	N/A	N/A		

Incident Summary

It was reported that when using AGFA-IMPAX (digital radiology imaging system software) staff can view sensitive data or his or her own medical information without seeing the usual warning notice.

Incident Update

08/28/11:
The software does not provide any warning when viewing a sensitive record, nor does it have the ability to audit access. All users of this software have the ability to view patient records even if it is a record that they do not have a need to view. The facility is looking into correcting this. Discontinuing use of the software would affect patient care.

09/02/11:
The IMPAX software does require its own separate logon after logging onto the VA network. It is deployed throughout the VISN but it is not used throughout the entire VA. It does have an auditing feature installed however it does not interface with VISTA. The staff who have been identified as the Picture Archiving Communication Systems (PACS) Manager have been trained on the security features.

09/07/11:
Since there is an auditing feature in the software, misuse of the software can be detected. The Data Breach Core Team (DBCT) suggested that the PACS Manager coordinate with the Information Security Officer and have reports run on a recurring basis to monitor for inappropriate activity.

Total number of Lost Blackberry Incidents	17
Total number of Internal Un-encrypted E-mail Incidents	69
Total number of Mis-Handling Incidents	81
Total number of Mis-Mailed Incidents	79
Total number of Mis-Mailed CMOP Incidents	6
Total number of IT Equipment Inventory Incidents	0
Total number of Missing/Stolen PC Incidents	4
Total number of Missing/Stolen Laptop Incidents	7 (4 encrypted)