



DEPARTMENT OF VETERANS AFFAIRS
Information Technology Field Operations
Field Security Operations
Network and Security Operations Center (NSOC)



Monthly Report to Congress of Data Breaches

July 5 - August 1, 2010

WARNING: This document is FOR OFFICIAL USE ONLY. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). This document is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel without prior approval of the Veterans Affairs Chief Information Officer. Where appropriate, U.S. person identities have been removed. Should you have a requirement for particular U.S. person identity information, contact the VA-NSOC. No portion of this report should be furnished to the media, either in written or verbal form.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0358339	Privacy	VISN 08 Miami, FL	7/6/10			High	1
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
7/6/2010	INC000000100174	N/A		N/A		N/A	0

Incident Summary

An employee placed an order for prosthetic equipment and printed a copy for Veteran A, but gave it to Veteran B. The form contained Veteran A's name, social security number and PHI.

Incident Update

07/07/10:
Veteran A will receive a letter offering credit protection services.

NOTE: There were a total of 90 Mis-Handling incidents this reporting period. Because of repetition, the other 89 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.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0358432	Privacy	VISN 15 Kansas City, MO	7/6/10	7/11/10		Moderate	1
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
7/6/2010	INC000000100224	N/A		N/A		N/A	0

Incident Summary

On 06/30/10, Veteran A called the Director's Office to report that he received Veteran B's information through the mail. Veteran A received a document which looked like an appointment reminder, but it also contained Veteran B's full name, full social security number, date of birth, gender and PHI.

Incident Update

07/07/10:
Veteran B will receive a letter offering credit protection services.

NOTE: There were a total of 103 Mis-Mailed incidents this reporting period. Because of repetition, the other 102 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 sent.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0359231	IT Equipment Inventory	VISN 07 Montgomery, AL	7/7/10			Low	
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
7/7/2010	INC000000100441	N/A		N/A		N/A	

Incident Summary

Five laptops were discovered missing during an annual IT equipment inventory at the Montgomery (East) campus. Four of the laptops were encrypted and one was an old BCMA laptop that was not encrypted. They were last accounted for between 01/01/09 and 06/30/09 and were in storage.

Incident Update

07/09/10:
According to the PO, there was no PII or PHI stored on the missing equipment.

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

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0360271	Privacy	VHA CMOPMURFREESBORO, TN	7/9/10	7/28/10		Moderate	0
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
7/9/2010	INC000000100874	N/A		N/A		N/A	1

Incident Summary

Patient A received medication information intended for Patient B. Patient B's name and medication type was compromised. Patient A reported the incident to the medical center. The Murfreesboro Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error.

Incident Update

07/09/10:
Patient B will receive a notification letter.

NOTE: There were a total of ten Mis-Mailed CMOP incidents out of 5,630,743 total packages (8,342,164 total prescriptions) mailed out for this reporting period. Because of repetition, the other nine 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 notification letter was sent.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0367291	Privacy	VISN 06 Richmond, VA	7/22/10			Moderate	
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
7/22/2010	INC000000103220	N/A		N/A		N/A	

Incident Summary

Human Resources (HR) reported that a call was received from an individual saying that her social security number was the same as one of our employees. OIG and the police have been notified.

Incident Update

07/23/10:

Per the OIG, a request was sent to the Department of Motor Vehicles and to the Social Security Administration for additional information. The picture ID from DMV may be received next week. Information has also been requested for HR to verify the employee's employment application.

07/29/10:

The caller's purse was stolen in 2008. She first became aware that someone was using her SSN when the IRS stated that she did not report all of her income for the 2008 tax year. Both the caller and the employee have the same name and SSN. Their dates of birth are off by one day. The employee had a background investigation done but it did not detect anything since it was a valid name and SSN match.

08/04/10:

Per the OIG, the employee is definitely using the wrong SSN. The question is why. The agent will interview the employee today or tomorrow. This is not considered a VA breach as the employee used this SSN on her employment application.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0370136	Privacy	VISN 10 Cleveland, OH	7/30/10			High	
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
7/30/2010	INC000000104641	N/A		N/A		N/A	

Incident Summary

The VA OIG and FBI are investigating an employee for threats and other issues. During a the investigation, OIG/FBI found two documents with patient identifiers from the VA in the employee's trash. Names, date of birth, home address and social security numbers were on the documents. The PO is opening an investigation to review the employee's access. There is a concern, based on a previous conviction of falsifying documents, that the employee may be inappropriately using patient information.

Incident Update

07/30/10:

The investigation is ongoing, and OIG would like the facility to review employee's access to patient records to see if any other inappropriate access is found.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0370620	Privacy	VISN 10 Columbus, OH	8/1/10			Moderate	0
Date US-CERT Notified	US-CERT Case Number	Date Privacy Notified	(Old)PVTS Number	Date OIG Notified	Accepted by OIG	OIG Case Number	No. of Loss Notifications
8/1/2010	INC000000104845	N/A		8/2/2010	No	Declined	1

Incident Summary

On 07/29/10, an individual (non-Veteran) called the pharmacy call center to report that he had erroneously received a prescription package meant for a Veteran. The information disclosed on the prescription package was the patient's name, medication name, instructions, and the caller's mailing address. The call center entered a message to the Columbus Outpatient Clinic via CPRS. The initial investigation found that the Veteran patient has changed his address seven times in the past year. The most recent address provided has belonged to the person who contacted call center for eight years. The caller stated that he does not know the Veteran. The caller then contacted a local TV station to report the incident. A local reporter contacted the Chief of Pharmacy to request an interview. There is an interview planned for the Pharmacy Chief with the reporter.

Incident Update

08/02/10:

The Chief of Pharmacy, Public Affairs Officer and Privacy Officer met with the local reporter. A written article was posted to nbc4i.com by 7:30 PM and the TV story aired on the local 11:00 PM news on 08/02/10. The story focused on wasting taxpayer money and on the frequency and number of pharmaceutical mis-mailings. On advice of Regional Counsel, the local facility did not provide numbers to the reporter but stated they would provide that information if the reporter submitted a written request. If questions are sent, the Public Affairs Officer will coordinate a response. Channel 4 had still photos and tape of the pharmacy packet and the person who called them. VA personnel inquired how they handled the security of information since they had a photo of the bottle which has the patient's full name. The news coverage blocked out the patient's name in the tape they ran with the story, however they did mention the name of the medication and that it was used for dementia patients.

This incident has been reported to OIG for further review. The PO is not able to contact the patient until his upcoming visit. The PO spoke with Regional Counsel and the Regional Public Affairs Officer.

08/04/10:

This incident has been declined by OIG. The Veteran patient will receive a letter of notification. He has an appointment tomorrow.

Resolution

The Privacy Officer has the signed notification letter to give to the patient if he shows up for his appointment today. If the patient does not show up, the PO will continue to monitor for an opportunity to hand off the letter since there is no valid address or phone number at this time.

Total number of lost Blackberry incidents	13
Total number of internal un-encrypted e-mail incidents	66
Total number of Mis-Handling Incidents	90
Total number of Mis-Mailed Incidents	103
Total number of Mis-Mailed CMOP Incidents	10
Total number of IT Equipment Inventory Incidents	3
Total number of Missing/Stolen PC Incidents	2
Total number of Missing/Stolen Laptop Incidents	6 (6 encrypted)

WARNING: This document is FOR OFFICIAL USE ONLY. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). This document is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel without prior approval of the Veterans Affairs Chief Information Officer. Where appropriate, U.S. person identities have been removed. Should you have a requirement for particular U.S. person identity information, contact the VA-NSOC. No portion of this report should be furnished to the media, either in written or verbal form.