

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
PSETS0000092928	Mishandled/ Misused Physical or Verbal Information	VBA St Petersburg, FL	8/5/2013	8/8/2013	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
VANSOC0595201	8/5/2013	INC000000303437	N/A	N/A	N/A	1	
Incident Summary							
Veteran A received a letter meant for Veteran B. The letter contained Veteran B's name, address, and SSN. Veteran A notified VA of the incident and returned the letter to us.							
Incident Update							
08/05/13: Veteran B will be sent 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 facility is unable to determine how violation occurred. The promo code was received and the credit protection letter was sent.							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000092967	Mishandled/ Misused Physical or Verbal Information	VISN 20 Seattle, WA	8/5/2013		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
VANSOC0595240	8/5/2013	INC000000303627	N/A	No	N/A	1	

Incident Summary

Personally Identifiable Information (PII), consisting of names, SSNs, financial information and other personal information belonging to two Veterans applying for benefits was given to a Veteran receiving an ID card. The information was released in the form of what was most-likely a benefit application. The incident happened on Friday, 08/02/13 at the Puget Sound Veterans Health Administration, Seattle. The recipient of the PII called one of the Veterans to inform him of the incident. This Veteran subsequently reported the incident to the Privacy Officer (PO).

Incident Update

08/06/13:

The two Veterans will be sent a letter offering credit protection services.

08/15/13:

The Veteran receiving the documentation on both Veterans made telephone contact with both Veterans immediately after it was discovered. Each Veteran acknowledged the fact that the recipient possessed the information. The Veteran possessing the information returned the documents to the Puget Sound Health Care System the next day as was promised to the two other Veterans. Both Veterans have the name, address and telephone number of the Veteran who received their PII. We are actively attempting to identify the individual releasing the PII at this time.

09/03/13:

Only one of the two Veterans can be identified by VA at this time.

NOTE: There were a total of 122 Mis-Handling incidents this reporting period. Because of repetition, the other 121 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.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000093079	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Leavenworth, KS	8/7/2013	8/9/2013	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
VANSOC0595347	8/7/2013	INC000000304373	N/A	N/A	N/A		1

Incident Summary

Patient A received a Medline Industries medical supply intended for Patient B. Patient B's name, address, and type of medical supply was compromised. Patient A reported the incident to the Fargo VA Medical Center and Patient B's medical supply has been replaced by Medline Industries. Leavenworth Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a Medline packing error. The packing error was reported to Medline for investigation and corrective action.

Incident Update

08/08/13:
Patient B will receive a HIPAA letter of notification.

NOTE: There were a total of 2 Mis-Mailed CMOP incidents out of 6,067,428 total packages (9,153,328 total prescriptions) mailed out for this reporting period. Because of repetition, the other 1 is not included in this report, but are included in the "Mis-Mailed CMOP Incidents" count at the end of this report. In both incidents, Veterans will receive a notification letter.

Resolution

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

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
PSETS0000093356	Mishandled/ Misused Physical or Verbal Information	VISN 19 Denver, CO	8/14/2013		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
VANSOC0595620	8/14/2013	INC000000306116	N/A	N/A	N/A		

Incident Summary

The Privacy Officer (PO) discovered 13 non-Veteran research participants who signed consents but did not sign HIPAA authorizations for a research sub-study. The non-Veteran patients' name, date of birth and the blood samples were sent to a research university for review.

Incident Update

08/21/13:

The PO is working on obtaining the HIPAA authorizations.

08/26/13:

The PO is working on obtaining the HIPAA authorizations on the 13 individuals, 9 non-Veteran and 4 Veteran. He may need the Institutional Review Board's (IRB) approval to send a letter to the patients. If that is the case, they are potentially looking at several weeks to obtain that approval then a few weeks to actually obtain signed HIPAA authorizations. If it is not the case, they can hopefully obtain signed HIPAA authorizations within two weeks.

08/27/13:

The Data Breach Core Team said that this should have already been reported to the IRB as a "protocol deviation." The IRB may choose to throw the 13 out of the study or to accept the retroactive authorizations. In either case, the researchers CANNOT use the data until the HIPAA authorizations are received.

09/03/13:

The study coordinator submitted a letter to Colorado Multiple Institutional Review Board (COMIRB) on 08/28/13 requesting to send to each participant asking them to return the enclosed HIPPA form to us at their earliest convenience. The coordinator was told by COMIRB this was an expedited protocol so we should have the approval in 2-3 weeks.

09/09/13:

The researchers know not to use the data until the HIPAA authorizations are received.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
PSETS0000093357	Mishandled/ Misused Electronic Information	VISN 18 Phoenix, AZ	8/14/2013		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
VANSOC0595621	8/14/2013	INC000000306121	N/A	N/A	N/A		

Incident Summary

On 08/14/13, the Privacy Officer (PO) reviewed copies of attachments to unencrypted email provided by the Chief of Staff (COS) which had been sent by a physician who is under review. The attachment content contained sensitive personnel material that was sent to a variety of internal staff and to a non-VHA email address. The non-VHA address correlated to the physician's attorney. The attachment also had a document that showed a non-VHA consultant's review of seven Veterans' medical cases including their last name and an in-depth medical summary. Other attachments included four other Veterans' identified cases. In part, this is due to copies of letters that the Veterans sent to the physician which includes their version of their medical issues and their home address or emails in addition to their full names. It is questionable from the content that the Veteran intended their letter to be distributed more widely than to the VA and/or the physician. Other materials attached contained de-identified Veteran cases which could be re-identified with reconstitution of medical information provided. There is also copious documentation regarding the physician's recounting of his professional encounters with his professional colleagues including his superiors. All materials described were sent unencrypted; however, of concern specifically is the Veterans' protected health information (PHI) to two non-VHA entities: an attorney and attorney/consulting firm. Disclosure of other information will also be referred to appropriate subject matter experts. Further notification and investigation, pending.

Incident Update

08/21/13:

In conversation with PO and Quality Safety and Improvement (QSI) yesterday, they indicated that the documents provided to HR for evidence file are not peer review and thus not 5705 protected. However, we intend to confirm visually via inspection in HR. The Chair of the Summary Peer review committee also believes the data provided to outside reviewers and attorneys includes this information PLUS supplemental medical records from the physician. Medical records were not provided to MD for this purpose nor did he consult with Privacy or his leadership. At this time, a PO is working with sources to fully identify the Veterans in this case. We will affirm or deny 38 USC 5705 shortly.

08/28/13:

The PO conferred with HR Assistant Chief. The materials were provided to the physician from the HR evidence file. This file had Veteran case history. HR redacted Veteran first name and first part of SSN. However, medical summaries of 9 Veterans were provided to the physician from the evidence file which included Veteran last name, last 4 of SSN, 1 case with "7332" information mentioned (marijuana use, continuous), the reviewing physician, their email work address, and reports of contact written by employees with full Veteran names. The summary cases were compiled in preparation for clinical review but were not labeled with "5705" protection nor was this exact documentation under the scope of peer review at the time compiled. As described previously, other Veteran materials in Veteran thank you cards or partial Veteran info with re-identifying info could be introduced.

09/04/13:

The COS is not the subject or the reviewer. The subject is a new surgeon who is undergoing disciplinary review. He was provided with case summaries of his patients. The surgeon sent those case files and possibly disclosed corresponding medical records for those cases to his attorneys and another consulting firm. He also disclosed personal thank you letters from Veterans written by them to VA. There were other cases, not part of the evidence file that he disclosed to his attorneys via emails. All unprotected PHI materials were provided to PO by COS and/or Chief of Surgery. The information was not 38 USC 5705 protected.

09/10/13:

This incident was discussed at the Data Breach Core Team meeting. Since the VA gave the information to the physician so that he could defend himself, he was within his rights to give it to his attorney to aid in his defense. He should not have sent it via VA email. This is a policy violation. No data breach occurred.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
PSETS0000093778	Missing/Stolen Equipment	VISN 22 San Diego, CA	8/23/2013	8/27/2013	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
VANSOC0596016	8/23/2013	INC000000308824	N/A	N/A	N/A		
<p>Incident Summary A VA Police Investigative Report was generated for one desktop and one laptop which were discovered missing during the Equipment Inventory List (EIL) 407 annual inventory conducted in June 2013.</p> <p>Both computers were utilized for brain imaging research. Psychology experiment programs which presented stimuli to research subjects would have been stored on the PCs. It was essentially presentation software. At no time did any of the experimental presentations access CPRS, VistA or any other program providing access to Personally Identifiable Information (PII), Protected Health Information (PHI), or VA sensitive information. The responsible party for the computers indicated that Microsoft programs (i.e. Word, PowerPoint, etc.) would have been installed and utilized for these presentations.</p>							
<p>Incident Update 08/26/13: This is an IT equipment inventory incident. The laptop was not encrypted. This was a research computer that only presented stimuli for psychological experiments performed during functional brain imaging studies. The computer was old and rarely used and was last seen more than a year ago. This computer was typically stored in a locked filing cabinet and was rarely used by any employee. The laptop was never connected to the VA network. It was never capable of being directly connected to the VA network.</p> <p>NOTE: There was 1 IT Equipment Inventory Incident this reporting period.</p>							
<p>Resolution There was no sensitive data stored on the equipment.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000094079	Unauthorized Electronic Access	WASHINGTON DC-NCA - 101 Washington, DC	8/30/2013		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
VANSOC0596310	8/30/2013	INC000000310528	N/A	N/A	N/A		

Incident Summary

Veteran's burial orders, which include the Veteran's DD214, are faxed to a service called MyFax using a VA provided toll free phone number. This service has several security concerns. MyFax service does not meet VA security requirements including co-mingling of data collected and placed in a zip file which is on an unsecure site. Data is downloaded by NCA. There is no media sanitization and no process for removing data that has been uploaded.

MyFax has stated, "If these are the requirements, we do not have any of these Gov't certifications and have never offered services on a segregated platform." There is no contract, SOW, or MOU that exists between VA, NCA, and MyFax. Services have been paid for since 2002 out of IT funds versus NCA funds.

Incident Update

09/09/13:

The faxes are sent in via an 800 number (by the family of the decedent) to the MyFax service. MyFax stores them and creates a file which they upload to a server. The NCA then runs a script that will retrieve the faxes from the server.

09/10/13:

This service was paid as a credit card purchase. The organization has written a Risk Based Decision memo and the ISO has provided her input on that for approval. The ISO is expecting to get the final version of that today.

Total number of Internal Un-encrypted E-mail Incidents	84
Total number of Mis-Handling Incidents	122
Total number of Mis-Mailed Incidents	103
Total number of Mis-Mailed CMOP Incidents	2
Total number of IT Equipment Inventory Incidents	1
Total number of Missing/Stolen PC Incidents	0
Total number of Missing/Stolen Laptop Incidents	7 (7 encrypted)
Total number of Lost BlackBerry Incidents	16
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	1