
DEPARTMENT OF VETERANS AFFAIRS
Office of Information & Technology
Office of IT Field Security Operations and
Office of Risk Management & Incident Response



Monthly Report to Congress of Data Incidents

December 5, 2011 - January 1, 2012

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000069304	Mishandled/ Misused Physical or Verbal Information	VBA Hartford, CT	12/5/2011	12/6/2011	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
	12/5/2011	INC000000185688	N/A	N/A	N/A	1	
Incident Summary							
Veteran A received a notification letter with a notification letter to Veteran B in the same envelope. Veteran A sent the mishandled letter to Veteran B and Veteran B reported the incident. The letter contained Veteran B's name, address and full SSN.							
Incident Update							
12/05/11: Veteran B will be sent a letter offering credit protection services.							
NOTE: There were a total of 58 Mis-Mailed incidents this reporting period. Because of repetition, the other 57 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							
Supervisors met with all staff involved with this incident and reinforced policies and procedures for mail handling.							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000069354	Mishandled/ Misused Physical or Verbal Information	VISN 16 Little Rock, AR	12/6/2011		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
	12/6/2011	INC000000185919	N/A	N/A	N/A	1	
<p>Incident Summary</p> <p>Veteran A was in the facility on 10/17/11 and he apparently received an appointment letter for Veteran B. Veteran A and Veteran B share the same last name and last four digits of their SSN. Veteran A received Veteran B's name, address and full SSN, as well as upcoming appointment information.</p>							
<p>Incident Update</p> <p>12/06/11: Veteran B will be sent a letter offering credit protection services.</p> <p>NOTE: There were a total of 85 Mis-Handling incidents this reporting period. Because of repetition, the other 84 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.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000069493	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Murfreesboro, TN	12/9/2011	12/20/2011	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
	12/9/2011	INC000000186628	N/A	N/A	N/A		1
<p>Incident Summary</p> <p>Patient A received a prescription intended for Patient B. Patient B's name and type of medication was compromised. Patient A reported the incident to the medical center and a replacement has been requested for Patient B. Murfreesboro Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error. The CMOP employee will be counseled and retrained in proper packing procedures.</p>							
<p>Incident Update</p> <p>12/09/11: Patient B will receive a letter of notification.</p> <p>NOTE: There were a total of 9 Mis-Mailed CMOP incidents out of 6,198,534 total packages (9,051,817 total prescriptions) mailed out for this reporting period. Because of repetition, the other 8 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.</p>							
<p>Resolution</p> <p>The CMOP employee was counseled and retrained in proper packing procedures.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000069526	Mishandled/ Misused Electronic Information	VISN 15 Kansas City, MO	12/9/2011		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
	12/9/2011	INC000000186728	N/A	N/A	N/A		

Incident Summary

VISN 15 has a contract with Compass Languages to provide language translation services for patients and their families. There is a Business Associate Agreement (BAA) and VA 6500.6 Appendix B and C security language is included in contract. A VA employee at Poplar Bluff VAMC questioned ftp upload of sensitive information to what they thought was company's website. Further investigation by the Information Security Officer (ISO) revealed that the contractor is using Cyberlynk.net to store translated patient information from CPRS. Compass Languages, VP, Client Relations stated in email that "when translating files the translation team uses their personal computers to perform the translation. Their personal computers contain glossaries, style guides and translation tools to aid in the translation process. Their personal computers are not Compass Languages owned." Additional email communication from Compass Languages Business Development Manager stated "All of our translators do not work within the United States. We use translators who are native speakers of the target language in order to ensure a high level of quality and accuracy within the translations. Sometimes those translators live inside the United States and sometimes they live in the target countries. All translators used for this contract sign Non-Disclosure Agreements with Compass Languages and all completed the VA Privacy/Security Training Module before beginning work on the files."

Incident Update

12/16/11:

Compass Languages provides face to face and telephonic language translation services, American Sign Language services, translation of written medical documents/instructions, etc. They provide services an estimated 3 - 5 times per week. The contract was awarded in September 2011.

Going forward, Compass Languages will only use translators and interpreters physically located within the United States. They will continue to require them to sign Non-Disclosure Agreements with Compass Languages and complete the VA Privacy and Security Training before commencing work. There are a number of solutions for the secure transfer and translation of files, and they are willing to work with VA technical staff to find a way to meet VA requirements and minimize cost. Additionally, their FTP server uses SSL (Secure Socket Layer) encryption during the transfer of files. SSL is the same type of encryption used in the HTTPS protocol.

12/23/11:

Instead of using personal computers, Compass Languages employees will use VPN access to the VA network where the contractor will access a SharePoint site to translate the documents. Each contractor who will need to access the VA network will have a background investigation done prior to being granted access to the network. This will also help ensure only US citizens will have access to patient information.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000069710	Mishandled/ Misused Electronic Information	VISN 04 Lebanon, PA	12/16/2011		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
	12/16/2011	INC000000187944	N/A	N/A	N/A		
<p>Incident Summary</p> <p>On 12/13/11, a Quinton field tech, Employee A replaced the PC for the Q-Tel system in the Physical Therapy (PT) area of building 102. He removed the entire PC to include the hard drive and sent it to their facility in Wisconsin. He was unaware of our policy for hard drive removal. He is now awaiting instructions for handling the hard drive.</p>							
<p>Incident Update</p> <p>12/16/11: The Information Security Officer (ISO) is trying to get the hard drive back however the company says VA will have to pay for it. The ISO is contacting the Contracting Officer to see what the contract says about who owns the hard drive. The data saved on the hard drive includes the name and last four digits of the SSN.</p> <p>12/19/11: The Q-Tel machine was under warranty and needed repaired. The company decided to replace the system in lieu of repairing it. I'm still trying to find out who purchased the system. The company said they will ship the hard drives back as soon as they receive payment for them.</p> <p>The Q-Tel is a respiratory medical device that is used in physical therapy. It tracks patient data to include last name and last 4 of SSN. Apparently it does not stay connected to the network, but does connect from time to time to upload that patient data.</p> <p>01/03/12: The facility opted to pay for the hard drives. The purchase order was completed and the Privacy Officer is waiting for the vendor to ship the hard drives.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE00000069792	Mishandled/ Misused Electronic Information	VHA Privacy Office (19F2) VHA CO (101) Washington, DC	12/19/2011		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
	12/19/2011	INC000000188383	N/A	N/A	N/A	4542	

Incident Summary

On 12/13/11, VHA was advised by VBA that an employee at the Fargo Region Office received a telephone complaint from the daughter of a Veteran whose name and social security number (SSN) was made public on Ancestry.com. The citation for the data source was "BIRLS Death File." The disclosure of the information was made by VHA FOIA Office pursuant to a FOIA request submitted by Ancestry.com. The disclosure contained 14.5 million Veteran records. The data included the Veterans' full name, SSN, date of birth, date of death, and up to three military branch assignments with entry and release dates.

Incident Update

12/19/11:

On 01/28/10, the VA FOIA Service within the Office of Information and Technology received the FOIA request from Ancestry.com. The organization requested "a complete copy of the VA database known as the Beneficiary Identification and Records Locator Subsystem (BIRLS) Death File (DF) - VBA System of Record 38VA21." Although initially assigned to VBA, the VBA FOIA Officer relinquished control of the FOIA request by transferring the request to the VHA FOIA Office with specific demands that VHA process the request due to VHA's familiarity with the data sources for the file being requested.

As part of standard operating procedures, the VHA FOIA Office is responsible for assigning each FOIA request to the appropriate program office for records search and retrieval of responsive records. During the week of 09/29/10 the responsive records were provided to the VHA FOIA Office on a DVD. Due to an unusually high volume of cases, the request was not responded to until 03/18/11, at which time the initial agency decision (IAD) letter with the responsive records enclosed was forwarded to the requester.

The authorized disclosure of the records was provided to the requester pursuant to FOIA. The disclosure of the information was completed under the guidance that all of the data maintained in the database was pertaining to deceased individuals. Although the release determination was based on the fact that the records pertained to deceased Veterans, there is no statutory authority for the disclosure of the names of the deceased Veterans under 38 U.S.C. 5701. Therefore, the names of the Veterans should have been withheld from the disclosure of the information.

There is no authority for the withholding of the SSN of a deceased individual. The disclosure of the deceased SSN is consistent with the disclosure of the same information by the Social Security Administration (SSA). Further, the Privacy Act does not apply to records on deceased individuals.

After receiving the complaint by VBA, preliminary data analysis indicates that approximately 5,000 of the names and SSN's provided to Ancestry.com belonged to living individuals. The VHA FOIA Office would have no means of validating data to determine which individuals were deceased and which were living. However, disclosure of the names and SSN's of such living individuals is considered a data breach under the Privacy Act.

12/20/11:

VBA staff generated the list of 5,223 individuals for whom VA could find no evidence of death in the most recent BIRLS file or VBA Corporate database; and provided the list to VHA. VHA will provide the list to Ancestry.com in a secure manner to permit them to take down the information on their website on these 5,223 individuals. Ancestry.com confirmed they were willing to remove the data from their site as soon as they receive and process the data from VA.

The Data Breach Core Team approved credit monitoring for the 5,223 individuals involved. VHA has agreed to send the letters.

12/21/11:

Analysis on the 5,223 individuals involved has begun, and duplicates have been found. After removing duplicates the new total is 4,542. At this time VBA has addresses for 3,757 of these. Ancestry.com has temporarily removed the "BIRLS Death File" from their website. If an Ancestry.com web page user had marked an entry in the user's family tree, the data still remains. If the end user attempts to review the source, he/she receives a message that the "BIRLS" Death File" is temporary unavailable.

01/05/11:

VA will provide a formal press release. The press release and credit monitoring letters are going through the concurrence process right now. OIT will sign the letters, which will be printed by the Hines ITC.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000069878	Mishandled/ Misused Physical or Verbal Information	VISN 20 Walla Walla, WA	12/21/2011		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
	12/21/2011	INC000000188911	N/A	N/A	N/A	72	
Incident Summary							
The door to fax/copy room was left open. The door opens into a high traffic patient area. The lockable lid on confidential disposal bin was left open and the items were accessible to anyone passing in the hallway							
Incident Update							
12/22/11: The Privacy Officer (PO) met with executive staff to discuss findings. The nurse executive called the Director to let him know what took place.							
01/03/12: The PO spoke with the supervisor of area where the documents were found. The tallying process is still being done.							
01/05/12: A total of 72 records had varying components of personally identifiable information (PII) that included full name, address, phone number, full social security number and protected health information (PHI). Therefore 72 Veterans will receive a letter offering credit protection services.							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000069887	Missing/Stolen Equipment	VISN 16 Little Rock, AR	12/22/2011		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
	12/22/2011	INC000000188985	N/A	N/A	N/A		
<p>Incident Summary</p> <p>Following an annual IT Inventory in which 99.8% of 13,646 items were accounted for, one workstation was discovered missing. In searching for the missing workstation, IT staff members were informed that heavy flooding occurred in Room 1N106-170-N a year ago. VA Police and Engineering staff reported to the site and stated that all of the equipment in the room was severely damaged. It appears that the workstation and monitor were removed without IT knowledge (no work order ticket issued) during the clean up. A search has been done as well as communications with all parties involved. No one knows what happened to the equipment nor who removed it. It is believed it may have been placed in an IT closet, but it has not been located.</p>							
<p>Incident Update</p> <p>12/22/11: The workstation was primarily used for administrative duties and to access VISTA/CPRS. There is no expectation that any sensitive data would be stored on the hard drive of this workstation. This was an IT equipment inventory error. No security breach has occurred.</p> <p>NOTE: There were a total of 2 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 1 is not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.</p>							

Security Privacy Ticket Number	Incident Type	Organization		Date Opened	Date Closed	Risk Category	
SPE00000070166	Mishandled/ Misused Physical or Verbal Information	VISN 09 Mountain Home, TN		12/29/2011		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
	N/A	N/A	N/A	N/A	N/A		79
<p>Incident Summary</p> <p>Per the Report of Contact (ROC) supplied by the Chaplain today: "I came into station on Saturday afternoon, 12/24/11 expecting to find my log book on the computer desk in the library located in the chaplain's office. Both library door and chaplaincy door were locked. My log book was not anywhere in the office. I cannot rule out the possibility that my memory is in error and that in fact the log book was not left in the library. The contents of the log book included the last name, last 4, and room number of every patient that I have visited since 10/11/11 through 12/23/11. With only a few exceptions, these were patients in the Nursing Home but did include some names and information from inpatients. The information included cover sheet personal data as well as my notes on the content of each visit/spiritual assessment, including some medical information. I am estimating that it would probably include 350 entries, and probably about 175 names.</p>							
<p>Incident Update</p> <p>01/03/12: An issue brief was completed per the Chaplain Service. A report was run for all of the patients seen by this Chaplain and per Chief Chaplain Service the update on the number of Veterans is that, "An estimated 79 patients may have been in the notebook."</p> <p>01/06/12: Seventy-nine patients will be sent notification letters.</p>							

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category		
SPE000000070200	Missing/Stolen Equipment	VISN 01 Bedford, MA	12/30/2011		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
	12/30/2011	INC000000189942	N/A	N/A	N/A		
<p>Incident Summary</p> <p>On 12/30/11 at 9:45 AM, a Research Administrative Officer noticed that the CPU from a VA desktop computer workstation was missing from Room B10-17. The main CPU was missing, but the cables and monitor were left in place. The user who reported it missing was not sure if the unit was stolen or relocated to another room so an initial search of nearby rooms was completed but did not provide evidence of the unit being relocated to another place. Information Resource Management (IRM) was contacted to see if they had moved the computer and they had not.</p> <p>The user who reported the CPU missing checked the Equipment Inventory List (EIL) 380 to see if this unit was a part of the research equipment listing. It was not. The computer and monitor were provided by IRM as a network workstation in B10-17. The missing unit was not yet connected to the VA network. The unit was not fully set up and only the initial VA image was on this device therefore, no sensitive data was stored on the computer.</p> <p>The VA Police were called immediately to file a report. A VA Police Officer came by to investigate. The user asked that IRM provide the make, model, EE and Serial number to the VA Police Officer for his Police report.</p>							
<p>Incident Update</p> <p>01/03/112: The Privacy Officer contacted the VA Police for an update. To date there is no further information to report.</p>							

Total number of Lost Blackberry Incidents	15
Total number of Internal Un-encrypted E-mail Incidents	73
Total number of Mis-Handling Incidents	85
Total number of Mis-Mailed Incidents	58
Total number of Mis-Mailed CMOP Incidents	9
Total number of IT Equipment Inventory Incidents	2
Total number of Missing/Stolen PC Incidents	3
Total number of Missing/Stolen Laptop Incidents	9 (9 encrypted)