
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

## December 30, 2013 - February 2, 2014

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Date of Initial DBCT Review |
|---|---|---|---|---|---|
| PSETS0000098522 | Mishandled/ Misused Physical or Verbal Information | VISN 09 Lexington, KY | 12/30/2013 | 1/2/2014 | |

| 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 |
|---|---|---|---|---|---|---|---|
| VANSOC0600613 | 12/30/2013 | INC000000335597 | N/A | N/A | N/A | | 1 |

**Incident Summary**

Veteran A received Veteran B's letter in the mail. The letter contained Veteran B's full name, address, diagnosis and patient record number. The letter was recovered. The incident involved one Veteran and was outside of VA control more than 72 hours.

**Incident Update**

12/30/13:
Due to the data elements exposed, the Incident Resolution Team (IRT) determined that Veteran B will be sent a letter offering credit protection services.

01/02/14:
The SSN was not exposed. Therefore the IRT determined that a HIPAA notification letter will be sent.

**Resolution**

The Privacy Officer (PO) re-educated staff on the proper handling of protected health information (PHI).

**DBCT**

12/30/13: No DBCT decision is required. This is informational for Mis-Mailed incidents and is the representative ticket. There were a total of 133 Mis-Mailed incidents this reporting period. Because of repetition, the other 132 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.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Date of Initial DBCT Review |
|---|---|---|---|---|---|
| PSETS0000098531 | Mishandled/ Misused Physical or Verbal Information | VISN 15<br>Kansas City, MO | 12/30/2013 | | |

| 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 |
|---|---|---|---|---|---|---|---|
| VANSOC0600620 | 12/30/2013 | INC000000335681 | N/A | N/A | N/A | | 1 |

**Incident Summary**

A Pharmacist self-reported accidently dispensing the wrong medication to Veteran A at the pick-up window. Veteran B who picked up the wrong medication was immediately notified per protocol, and asked to return it to pick-up the correct medications. Veteran B' name and medication information was compromised.

**Incident Update**

12/30/13:
Due to the data elements exposed, the Incident Resolution Team (IRT) determined that Veteran B will be sent a HIPAA letter of notification.

**DBCT**

12/30/13: No DBCT decision is required. This is informational for Mis-Handling incidents and is the representative ticket. There were a total of 112 Mis-Handling incidents this reporting period. Because of repetition, the other 111 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 | Date of Initial DBCT Review |
|---|---|---|---|---|---|
| PSETS0000098564 | Missing/Stolen Equipment | VISN 11 Detroit, MI | 12/31/2013 | 2/10/2014 | 1/7/2014 |

| 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 |
|---|---|---|---|---|---|---|---|
| VANSOC0600655 | 12/31/2013 | INC000000335855 | N/A | N/A | N/A | | |

**Incident Summary**

Six data storage medical devices were unable to be located during an Equipment Inventory Listing (EIL) inventory upon an employee separation from the facility.

**Incident Update**

12/31/13:
The Chief Logistics Officer (CLO) is working to get copies of the VA Police reports now. There were several items missing during the annual certification for the EIL, so as soon as she receives a Report of Survey (ROS) for sensitive items, she notified the Information Security Officer (ISO). The CLO is working to get all the information and verify the accuracy of such information.

01/02/14:
It is the opinion of the covering ISO that this equipment was most likely either already turned in or relocated without the location updated. It may take a few days to locate all of the equipment. Staff in Detroit is investigating the missing equipment.

01/03/14:
The CLO has spent the last two days trying to verify information, review work orders to see if these devices have been serviced by Biomed, and getting the Police reports. In the past 24 hours they have located two laptops and are still trying to make certain that the items are truly missing.

01/09/14:
Some of the missing equipment listed includes 2 laptops, 2 tablets, and 4 wireless nursing phones. No Blackberry phones were on the list. They were not encrypted because they were older devices.

All the laptops and tablets were found and 1 of the phones was found. They following are still missing according to the latest Police report (01/02/14). Some of these may have been found yesterday.
Bar code scanner
Vital signs monitor(2)
Wireless nursing phones(3)
VCR player (1)
Printer, color-laser jet(4)
Scanner (1)
Human touch robotic massager (1)

01/10/14:
An updated ROS was attached to the ticket. All the lost computers and laptops have been found. The ISO spoke to the Administrative Officer of the Day (AOD) of Radiology yesterday and 14 of the 16 pieces of equipment missing were found.

01/23/14:
Only 2 items are still unaccounted for on the equipment list. They are an i-Site radiology workstation (the ISO is not sure if it's a monitor or a workstation) and an ultra sound machine. They are still searching for the equipment.

02/03/14:
The ROS was sent back to the service to find the 2 remaining items. It is doubtful that there is any personally identifiable information (PII) on the devices. The service is still looking for the equipment.

02/12/14:
The ultrasound was at the facility on a trial and demonstration and it is believed that it was returned to the sender. The ISO is still awaiting confirmation from the vendor. According to AMS-MERS (our inventory software), the i-Site workstation is in the facility somewhere, but not where it is supposed to be, so they will keep looking.

**Resolution**

The Report of Survey has been completed. The ISO is waiting for the AD signature on the ROS.

**DBCT**

12/31/13: No DBCT decision is required. This is informational for IT Equipment Inventory incidents and is the representative ticket. 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 is included in the "IT Equipment Inventory Incidents" count at the end of this report.
01/07/14: The DBCT reviewed and wanted to know what the six devices are and whether they are encrypted or not.
01/14/14: The DBCT was informed of the types of devices missing.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Date of Initial DBCT Review |
|---|---|---|---|---|---|
| PSETS0000098582 | Mishandled/ Misused Physical or Verbal Information | VHA CMOP Hines, IL | 12/31/2013 | 1/21/2014 | |

| 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 |
|---|---|---|---|---|---|---|---|
| VANSOC0600673 | 12/31/2013 | INC000000335921 | N/A | N/A | N/A | | 1 |

**Incident Summary**

Patient A received Patient B's prescriptions. Patient B's name, type of medication and address was compromised. A Consolidated Outpatient Pharmacy (CMOP) Business Associate who pre-sorts CMOP prescription packages prior to being placed in the mail stream labeled the package with Patient A's address. This incident has been reported to Parcelite for internal investigation and corrective action. UPS has been notified to return the package to the CMOP.

**Incident Update**

12/31/13:
Based on the protected health information (PHI) exposed, including name, address and medication information, the Incident Resolution Team (IRT) determined that Patient B will receive a HIPAA letter of notification.

**Resolution**

This incident was reported to Parcelite for internal investigation and corrective action. UPS has been notified to return the package to the CMOP.

**DBCT**

01/07/14: No DBCT decision is required. This is informational for Mis-Mailed CMOP incidents and is the representative ticket. There were a total of 6 Mis-Mailed CMOP incidents out of 7,720,362 total packages (11,404,886 total prescriptions) mailed out for this reporting period. Because of repetition, the other 5 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 | Date of Initial DBCT Review |
|---|---|---|---|---|---|
| PSETS0000098932 | Missing/Stolen Equipment | VISN 02 Buffalo, NY | 1/10/2014 | 1/10/2014 | |

| 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 |
|---|---|---|---|---|---|---|---|
| VANSOC0601008 | 1/10/2014 | INC000000337936 | N/A | N/A | N/A | | |

**Incident Summary**

VA Western New York HealthCare System (WNYHCS) VAMC Research Department turned in a laptop for hard drive removal and disposal to the local WNYHCS IT Department. WNYHCS local IT Department discovered there was not a hard drive in the laptop.

**Incident Update**

01/10/13:
Per the Information Security Officer (ISO), the Research Administrative Officer (AO) advised that the laptop in question was last inventoried in 2011. The researcher and co-investigator researchers who was last listed as being in possession of the laptop advised that they do not know what happened to the hard drive and that they do not remember being in possession of the laptop. The Research AO advised that the local research non-profit purchased the laptop and they advised that no sensitive VA data was stored on the laptop. The Research AO cannot verify if the laptop was encrypted. The local IT Department has no record of the hard drive being turned-in. The local IT Department has no record of the laptop ever being encrypted. The local ISO audited hard drives that have been degaussed and destroyed and did not find the hard drive listed as having been destroyed. The Research AO is in the process of contacting the researcher last listed as being in possession of the laptop to see if any more relevant information regarding the whereabouts of the hard drive can be obtained.

Per the researcher, no information at all was ever entered into the laptop. It was intended to be used to complete case report forms. Case report forms, once filled out were not able to be saved; only printing is allowed. The research coordinator never entered research information or patient information into the laptop. There is no Information Resource Management (IRM) record that this laptop was encrypted so encryption cannot be verified.

**Resolution**

WNYHCS VAMC has implemented a corrective action plan to identify, inventory and encrypt all research laptops.

**DBCT**

01/14/14: No DBCT decision needed. This stays on as informational for missing equipment.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Date of Initial DBCT Review |
|---|---|---|---|---|---|
| PSETS0000099240 | Mishandled/ Misused Electronic Information | Corporate Data Center Operations (CDCO) Austin, TX | 1/16/2014 | | 1/22/2014 |

| 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 |
|---|---|---|---|---|---|---|---|
| VANSOC0601290 | 1/16/2014 | INC000000339319 | N/A | N/A | N/A | 1510 | 145 |

**Incident Summary**

On 01/15/14, around 10:00 PM, approximately twenty Veterans (Veteran A) called a VA Help Desk and reported they were able to see another Veteran's (Veteran B) information when they logged on to eBenefits. At this time it is known that Veteran's B name and mailing address were visible. Veteran A was able to access any of the information available in eBenefits for Veteran B, but it is unknown if Veteran A moved past the initial welcome page. VA IT Specialists are investigating whether or not logs can be pulled showing which pages were accessed. Approximately 10,000 users logged in to eBenefits on 01/15/14 so IT Specialists are investigating in attempt to narrow the time frame of when the incident began and ended. This ticket will be updated as information is received. NSOC opened a separate Remedy ticket to address the security issues. They did not create a PSETS ticket which is why this PO created this ticket. The NSOC ticket is VANSOC0601263.

01/18/14 7:52 PM: Update to the incident description.
VA Authentication Federation Infrastructure (VAAFI) was patching servers located at Terramark, without notification to Enterprise Operations (EO) or National Service Desk (NSD) when Veterans began contacting the eBenefits (EBN) Help Desk with reports of seeing other Veterans PII information being produced on their screens. The incident started being reported on 01/15/14 about 9:00 PM ET. The NSD was notified on 8:43AM ET on 01/16/14.

**Incident Update**

01/16/14:
The time frame of the incident is from 01/15/14, 8:03 PM 01/16/14, 12:56 AM. During this time 10,154 users logged on to eBenefits. Of this number, 5,351 users potentially saw another user's information or their own data was exposed. eBenefits was taken off-line on 01/16/14 at 8:20 AM. It was back online at 10:15 AM. It was taken off-line a second time at 10:47 AM and remains off-line. The investigation is continuing. A Swift Action and Triage (SWAT) team was convened by 8:53 AM.

01/17/14 9:46 AM:
The SWAT call ended yesterday around 5:30 PM.

01/17/14 4:32 PM:
The PO sent the following request to NSOC. If EBN users call into a help desk to report issues that involve security and privacy issues and a new Remedy ticket is created for every call, can they assign the ticket to the Austin PO and ISO? The PO's concern is if an ISO creates a ticket and she is not paired with the ticket in Remedy, she won't know the ticket exists. And if the person is reporting new information, the PO's updates to the Incident Resolution Team (IRT) will not be accurate. The IRT will be pulling information from this ticket for some of their reports and meetings.

01/18/14 11:03 AM:
As of the 8:00 AM call today, the eBenefits team is still reviewing logs to determine what type of data was exposed. They are reviewing logs on the 5,351 users so it is not a quick process. We know there is no protected health information (PHI), and the last 4 of the SSN were visible.
In the review, they noticed that form 21-22 (Request for Representation) was submitted at 10:00 PM on 01/15/14. They can tell the form was opened at 10:00 AM on 01/15/14 by the Veteran, and this was before the incident timeframe. So chances are very good that the Veteran was the submitter, but the only way to know for certain is to contact the Veteran. The SWAT team is trying to locate someone from a help desk who can contact the Veteran. The person will be provided with a script to follow and someone else will also be on the line to coach if necessary. They are aware they cannot ask the Veteran for personally identifiable information (PII) nor can they mention any PII since we are calling the Veteran.

eBenefits may be brought back up at 11:00 AM today (not sure what time zone). The help desk number listed on the eBenefit site for users to call is closed on weekends. The PO recommended that we have a service desk available for calls considering the circumstances. They agreed and will see if it's possible to reroute the calls to the National Service Desk (NSD) number. If not, they will put a banner on the website with a number for users to call if they have issues. The PO provided them with a script field security sent me yesterday. NSD management is reviewing it now and will make necessary changes.

01/18/214 7:55 PM:
Update to information discussed during the SWAT call on 01/16/14:
o Still waiting on data from DMDC so that we can create the letters and notifications to Veterans.
o Features that are a part of the new EBN functionality: Payment History, Letter Generation, Claims Status; determined that PHI was not in any of these options.
o It hasn't been determined if the affected records could be changed/manipulated. Logs are still being reviewed.
o 21 security breach tickets were reported by the EBN Help Desk.

01/18/14 8:01 PM:
Update to information discussed during the SWAT call on 01/17/14:
o The final number of users affected is not identified, will fall between 4731 and 5351.
o Approximately 1,200 users had their data exposed with 5,351 who could have viewed the data.
o A user opened the form 21-22, Request for Representation, at 10:00 AM on 01/15/18 (before the incident time frame). The form was submitted at 10:00 PM on 01/15/14. It is a strong probability that the Veteran was the submitter, but the only way to verify is to contact the Veteran.
o The number of users affected is staying in the 5,351 range. The team is still reviewing audit logs for each click made by the user, working to get the total number of users with their data exposed; no commitment to numbers yet, need to finalize and review work.
o A local news station covered the incident and interviewed a Veteran who brought letters they stated were printed off eBenefits, some for other Veterans. The entire pages of the letters were not visible on the broadcast so it cannot be said for certainty they were all from eBenefits. The data seen on the broadcast was: last four of the SSN, full name, address, bank name, last four number of a bank account, disability percentage awarded, disability effective date, and the disability compensation total/monthly amount.
o Payment history has no download capability but can be printed.
o Letter generator produces a system generated letter that can be screen printed.
o Claims status has no download capability but can be printed.
o Validation is required on whether or not any of the following information is presented in any of the eight generated letters: full SSN, DOB, or full bank account number.
o Need to find out whether or not changes can be made to any of the data.
o 26 Veterans called the NCC helpdesk.

01/18/14 9:29 PM
Summary of information discussed during the SWAT call on 01/18/14:
o The VA has not contacted the Veteran yet. Management is still trying to locate someone from a help desk to contact the Veteran.
o Have not verified that the number of users is 4,731. It is highly likely they will stay with 5,351.
o eBenefits remains off-line because the help desk that receives calls from eBenefit users is closed on the weekends. Leadership is looking in to this to issue.
o The logs for all 5,351 are being reviewed, which is a lengthy process.

01/19/14 9:23 AM:
Below is a summary of the calls that have occurred thus far today. The PO will continue to add to this email as the day proceeds.
7:00 AM CT Call:

VBAVACO is going to assist in contacting DoD on data the VA may need, and to ensure DoD is ready to go live at 10AM ET.

Testing is showing going well. There is one unusual finding, dates on a DD214. The problem is not with EBN, it's a back end portal with three other systems and this is a pre-existing problem. It may show a date with nothing else after it, so it looks incomplete. No other issues in testing were found.

A banner has been added to the EBN front page which will direct users to National Call Center (NCC) help desk.

When a Veteran submits a claim, and it is in pending state, they are able to upload documents. During the timeframe of the incident, 13 users, uploaded a total of 63 documents. Veterans cannot view, delete, download or alter in anyway documents after they have been uploaded. The EBN team is reviewing the documents for identifiable data to pair with the correct Veterans account. There may be a chance that a document does not have identifiable data since a Veteran can upload anything, such as a smiley face. If this occurs the VA may need to call the Veteran to ensure the correct documents are placed in the correct account. The NCC help desk has an employee working today who is able to contact Veterans.

The NCC Help Desk has 10 agents and will be open 10:00 AM-5:00 PM ET today. Depending on how day goes today, they will be open 10AM-5PM ET on 01/20/14. The help desk is waiting on the final version of scripting to use when speaking to Veterans.
7:50 AM CT Call:

The team that was assigned to review the 63 documents has only found 19. This does not impact the go live time as the documents are not accessible to Veterans anymore. The EBN team will work with the other team on locating the documents.

All teams are in concurrence to a go live time at 10:00 AM ET for EBN.

01/19/14 10:44 AM:
Summary of 8:50 AM CT SWAT call:
- o eBenefits was back online at 10:00 AM ET with a banner directing users to the help desk.
- o Within 6 minutes of being online there were 715 users logged in to eBenefits. No issues seen by administrators so far.
- o By 10 minutes after, 1029 users were logged in.
- o By 20 minutes after, 2100 users were logged in. EBN is running optimally at this time.
- o Teams will continue to monitor logs for number users logged in and if any issues arise.

01/19/14 11:26 AM:

10:35 AM ET: The help desk reported receiving 35 calls, no outstanding issues reported.

11:10 AM ET: Possible surge at 11:30 AM ET due to public affairs announcing eBenefits is back online.

24,080 users logged in at this time.

01/19/14 7:10 PM:
Those working IT have one more checking in at 7:55 PM ET before the 8:00 PM ET Leadership meeting. They have not said yet when to call in tomorrow. The PO will need to check the whiteboard on the live meeting later tonight for the time.

Summary of 4:00 PM CT SWAT call:

The NCC help desk closed at 5:00 PM ET. They received a total of 236 calls and no issues were reported. One person called stating they viewed another person's data when logged in to EBN on the evening of 01/15/17. This occurred during the incident timeframe.

Because EBN is operating without issues the help desk will be closed tomorrow (01/20/14) and reopen on 01/21/14. If there is an issue with EBN overnight or during the day tomorrow the help desk can open.

The Veteran who had form 21-22, Request for Representation, in their file was called yesterday by a VA employee. The Veteran confirmed that he had submitted the form on the evening of 01/15/14. So no incident occurred in this situation.

01/20/14 10:55 AM:
Summary of 9:00 AM CT SWAT call:

EBN group tasked with updating Privacy on that status of the 13 claims with 63 documents uploaded in EBN on the time of the incident. They continue to attempt to pair the documents with the correct claimant.

Office of Business Process Integration (OBPI) and others are tasked with providing Privacy the mailing addresses for the 5,351 EBN users.

Next call is at 9:00 AM ET 01/20/14. The call line will remain open. The whiteboard in the on-line meeting will remain up for people to added updates. The SWAT team needs to continue to monitor emails in case a call is scheduled for today.

01/21/14 11:28 AM:
This morning we met briefly at 9:00 AM for last check-in. No new information was covered. It was determined that the SWAT call is no longer needed. The EBN group is still reviewing logs in order to advise what type of data was visible. They are also compiling a list of the 5351 users and their mailing addresses. Some of the information will need to come from DoD. This morning the POI received 6 Reports of General Information from ISOs. When EBN users called a help desk to report viewing another person's data (all occurred during incident time frame) the help desk created a report and sent to their ISO. Some ISOs must be back in the office today as this PO is beginning to receive them. NSOC stated a new Remedy ticket must be opened for every caller. The initial ticket will not cover it. The PO will begin creating tickets and reference the initial one created on 01/16/14.

01/22/14:
This ticket was discussed at the Data Breach Core Team (DBCT) meeting today. Several SWAT team members joined the call. It was determined that the 5,351 did not represent the total number of Veterans whose information was compromised, but rather the 5,351 represents the total of Veterans online at eBenefits during the time frame in which the incident occurred. The SWAT team members are still working to determine the total number of Veterans whose information was compromised and the exact data elements that were compromised. They estimate that this number would be closer to 1,200. They plan to have the final number and the data elements that were compromised by COB 01/23/14.

01/27/14:
This PO is still waiting for the final number of the Veterans affected by this incident and the exact data exposed. This PO has emailed the individuals collecting the information several times and is still waiting on a response.

Here is what they have identified as personally identifiable information (PII) from the Electronic Claim Submissions: Name, Address, Phone number, SSN, Date of Birth, Email, Spouse name, Spouse SSN, Spouse DOB, Spouse address, Child name, Child SSN, Child DOB, Child Address, Spouse's Previous Marriage (Names), Insurance account number, Disability rating, Hospital addresses/stays.

01/28/14:
The DBCT is still waiting for the final count and the specific data elements. The 1,362 may or may not include the spouses' and dependent children's' information. We also need a breakdown of the minor children's' information so that ID Analytics can provide web crawling surveillance.

01/29/14:
The final count of those whose information was exposed is 1,362. There were 199 dependent children, 146 are under 18 years of age. Therefore, 1,216 will receive letters offering credit protection services and the information on the 146 dependent children under 18 will be sent to ID Analytics for web crawling surveillance.

01/30/14:
Additional review indicates that of the 199 dependents identified, 49 are adult dependents, leaving 150 children under the age of 18. The number of adults whose information was exposed is 1176. The 1176 individuals will receive letters offering credit protection services and the 150 dependent minor children's information will be sent to ID Analytics for web crawling surveillance.

02/04/14:
There are five dependents without SSN's. VBA stated the children do not have SSNs in the corporate database and the only valid way to acquire their SSNs would be through requests to the Veterans. This PO emailed the Director, IRT and asked if the list should be provided as is to VA Identity Safety.

The two template letters have been approved by the Director, Incident Resolution Team (IRT). One template is for adults and the other is for the dependents of the adults. This PO provided VA Privacy Service with names, addresses and promo codes for three adults. VA Privacy Service will have the Deputy Assistant Secretary for Information Security sign the letters before mailing them today. This PO notified those from OBPI and VBA who are working on the lists of names and addresses to remove the three names and promo codes which were provided to VA Privacy Service today.

The list of adults is missing information on approximately sixty individuals. OBPI and VBA are searching other systems and trying other avenues to gather the information.

This PO has a conference called scheduled for the morning of 04/05/14 to discuss the printing and mailing.

02/06/14:
During the preparation of test files for the print group it was discovered that the 1362 total is incorrect. The total number of affected Veterans, Servicemen, spouses and children is 1655, a 293 increase. When compiling the overall list, a majority of the dependents were not included in the count. A total of 285 more promo codes are needed.

The PO previously mentioned that there were 60 individuals they were searching for mailing addresses on. They have found 55. So of the 1655, we can print and mail 1650 of the letters.

The paragraph below is in the letters to the adults and dependents under 18.

On 01/15/14, during a process to improve software supporting the joint VA and Department of Defense (DoD) benefits web portal (eBenefits), VA discovered a software defect. On that day, some Veterans, Servicemen and dependents that registered and logged into eBenefits were able to see a combination of their own information as well as data from other eBenefits users.

02/14/14:
The Privacy Officer reports that the letters were delivered to the Post Office on 02/14/14 for mailing.

**DBCT**
01/22/14: The DBCT wants to know the number of individuals involved and the data elements that were exposed.
01/28/14: The DBCT is still waiting for the final count and the specific data elements. The 1362 may or may not include the spouses' and dependent children's' information. We also need a breakdown of the minor children's' information so that ID Analytics can provide web crawling surveillance.
02/11/14: The total number of affected Veterans, Servicemen, spouses and children is 1655, a 293 increase. When compiling the overall list, a majority of the dependents were not included in the count.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Date of Initial DBCT Review |
|---|---|---|---|---|---|
| PSETS0000099406 | Mishandled/ Misused Electronic Information | VISN 17 San Antonio, TX | 1/21/2014 | | 1/22/2014 |

| 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 |
|---|---|---|---|---|---|---|---|
| VANSOC0601437 | 1/21/2014 | INC000000340324 | N/A | N/A | N/A | 143 | |

**Incident Summary**

A GE Stress Test Machine with CPU and Monitor was sold as scrap to an individual. He stated once he was able to get it to work, he had access to a patient list (approximately 163 individuals). The Privacy Officer (PO) will know the exact count once Biomed retrieves the data. The machine has been returned and in Logistics' possession.

**Incident Update**

01/28/14:
The DBCT determined that 143 letters offering credit protection services will be offered.

It was sent out without being wiped because of lack of adherence to the media sanitization policy. The person who bought the machine was a vendor. The individual used the default password which had never been changed. The person viewed the information and recognized what it was then returned the device. The DBCT determined that 143 letters offering credit protection services will be sent.

**DBCT** **DBCT Decision Date:** 1/28/2014

01/28/14: It was sent out without being wiped because of lack of adherence to the media sanitization policy. The person who bought the machine was a vendor. The individual used the default password which had never been changed. The person viewed the information and recognized what it was then returned the device. The DBCT determined that 143 letters offering credit protection services will be sent. This stays on as informational due to the number of patients affected.

| | |
|---|---|
| Total number of Internal Un-encrypted E-mail Incidents | 77 |
| Total number of Mis-Handling Incidents | 112 |
| Total number of Mis-Mailed Incidents | 133 |
| Total number of Mis-Mailed CMOP Incidents | 6 |
| Total number of IT Equipment Inventory Incidents | 2 |
| Total number of Missing/Stolen PC Incidents | 0 |
| Total number of Missing/Stolen Laptop Incidents | 0 |
| Total number of Lost BlackBerry Incidents | 23 |
| Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents | 3 |