

Information Security Monthly Activity Report*

April 2015

VA uses a defense-in-depth approach to information security to protect the data we hold on Veterans. While the defense-in-depth approach protects from inbound threats and contains other data exposing incidents, VA relies on employees to protect Veteran information they handle and transmit. This graphic demonstrates how the layered defense protects Veterans from threats, and where data exposures have occurred for the past month.

Threats Blocked or Contained By VA's Defense In Depth



0 VETERANS AFFECTED

- 0 Notifications
- 0 Credit Protection Services Offered

Of the total # of Veterans affected, 0 were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



Intrusion Attempts (Blocked)
308,390,065



Malware (Blocked/Contained)
956,449,158



Suspicious/Malicious Emails (Blocked)
52,939,418



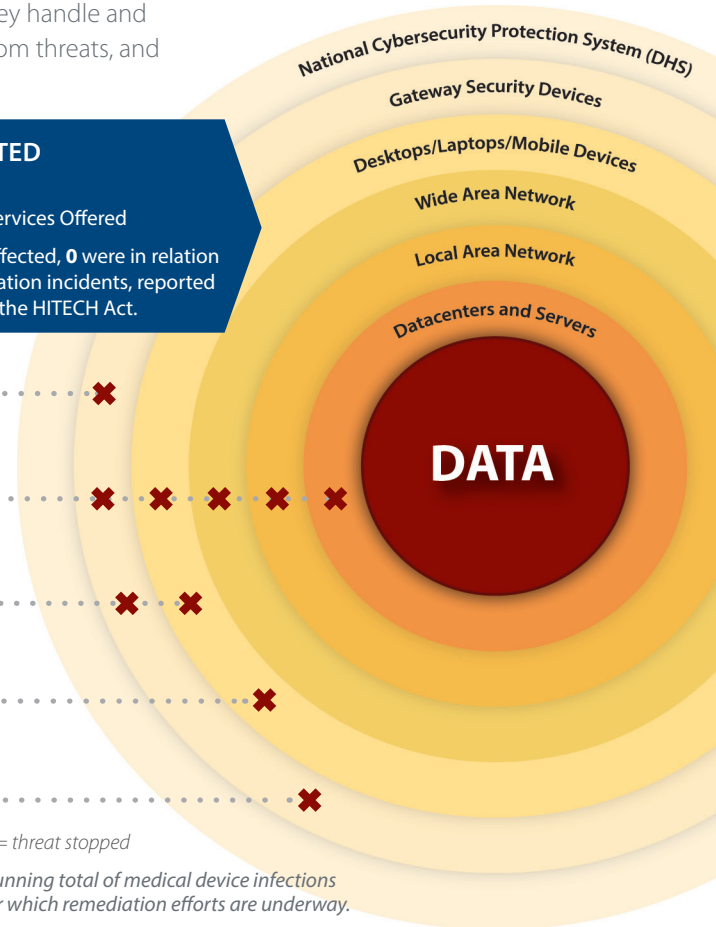
Infected Medical Devices (Contained)**
2



Outgoing Unencrypted Emails
93 Associated Privacy/Security Events
16,626 Total Emails Blocked

✘ = threat stopped

** Running total of medical device infections for which remediation efforts are underway.



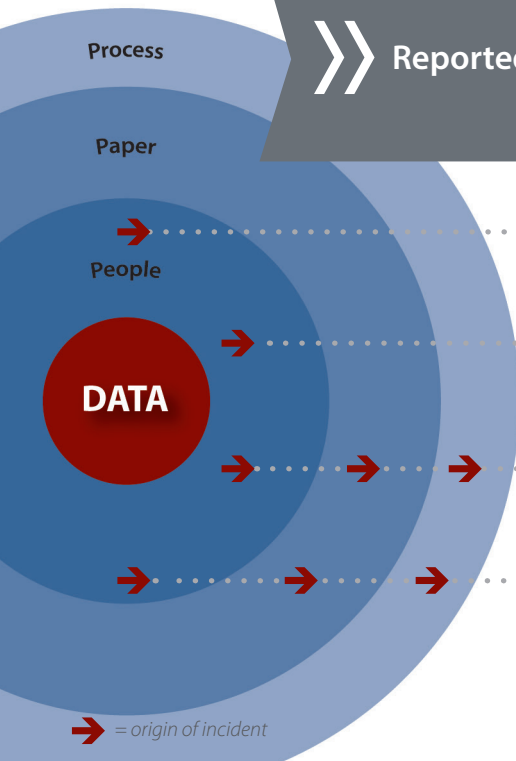
Reported Events



987 VETERANS AFFECTED

- 398 Notifications
- 589 Credit Protection Services Offered

Of the total # of Veterans affected, 738 were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



Lost and Stolen Device Incidents
47



Lost PIV Cards
144



Mishandled Incidents
112



Mis-mailed Incidents
204 Paper Mis-mailings

3 Pharmacy-item Mis-mailings
out of **7,307,142** Total Mailings

→ = origin of incident

*This graphic is a visual depiction of VA's information security defense in depth. It is not intended to provide an exhaustive summary of VA's information security activity. This data, which is extracted from Data Breach Core Team and US-CERT reporting, represents a snapshot in time and is subject to change based on further validation.

DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Incident Resolution Service

Monthly Report to Congress of Data Incidents

April 1-30, 2015

Security Privacy Ticket Number: PSETS0000117649
DBCT Category: IT Equipment Inventory
Organization: VISN 04
Coatesville, PA
Date Opened: 4/6/2015
Date Closed: 4/10/2015
Date of Initial DBCT Review: N/A
VA-NSOC Incident Number: VANSOC0619174
Date US-CERT Notified: 4/6/2015
US-CERT Case Number: INC000000457033
US-CERT Category: Category 1 - Unauthorized Access
No. of Credit Monitoring:
No. of Loss Notifications:

Incident Summary

The facility Chief Information Officer (CIO) reported the loss of 31 items on the annual IT inventory. Only four desktop PCs and two network switches were capable of holding data once power was removed. Office of Information and Technology (OI&T) staff reported the four desktop computers were encrypted and the two network switches were still in the box from the manufacturer and not programmed for use.

Incident Update

04/06/15:

The Incident Resolution Service Team has determined that no data breach has occurred. The PCs are encrypted.

Resolution

A VA Police report was filed and an investigation was started on 04/03/15.

DBCT Decision Date:

DBCT

This incident was discussed by the DBCT, but no DBCT decision is required. This is informational for IT Equipment Inventory incidents and is the only IT Equipment Inventory Incident is reporting period.

Security Privacy Ticket Number: PSETS0000117908

DBCT Category: Mishandling

Organization: VBA
Washington, DC

Date Opened: 4/10/2015

Date Closed:

Date of Initial DBCT Review: 4/14/2015

VA-NSOC Incident Number: VANSOC0619421

Date US-CERT Notified: 4/10/2015

US-CERT Case Number: INC000000458285

US-CERT Category: Category 6 - Investigation

No. of Credit Monitoring:

No. of Loss Notifications: 173

Incident Summary

Transit applications that were sent to VBA Central Office (CO) for processing were misplaced at VBA CO.

Incident Update

04/15/15:

They were sent UPS 2nd Day Air.

04/21/15:

The package was received at the Huntsville mail intake center. This is a secured area. It has not been located at this point. The transit applications include employees' full names and last four numbers of their social security numbers, addresses, and phone numbers.

05/05/15:

The DBCT has determined that a data breach has occurred, and that all 173 employees will be sent general notification letters.

DBCT Decision Date: 05/05/2015

DBCT

The DBCT determined that a data breach has occurred since the documents cannot be found.

Security Privacy Ticket Number: PSETS0000117976
DBCT Category: CMOP Mismatched
Organization: VHA CMOP
Charleston, SC
Date Opened: 4/13/2015
Date Closed: 4/20/2015
Date of Initial DBCT Review: N/A
VA-NSOC Incident Number: VANSOC0619483
Date US-CERT Notified: 4/13/2015
US-CERT Case Number: INC000000458915
US-CERT Category: Category 6 - Investigation
No. of Credit Monitoring:
No. of Loss Notifications: 2

Incident Summary

Patient A received prescriptions intended for Patient B and Patient C. Patient B's and Patient C's name and type of medication were compromised. Patient A reported the incident to the Salisbury VA Medical Center and a replacement has been requested for Patient B and Patient C. Charleston Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error.

Incident Update

04/13/15:

The Incident Resolution Service Team has determined that Patient B and C will be sent HIPAA notification letters due to Protected Health Information (PHI) being disclosed.

Resolution

On 4/13/15, the CMOP employee was counseled and retrained in proper packing procedures.

DBCT Decision Date:**DBCT**

No DBCT decision is required. This is informational for Mismailed CMOP incidents and is the representative ticket. There were a total of 3 Mismailed CMOP incidents out of 7,307,142 total packages (10,361,640 total prescriptions) mailed out for this reporting period. Because of repetition, the other two incidents are not included in this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number: PSETS0000117990
DBCT Category: Mismatched
Organization: VISN 06
Durham, NC
Date Opened: 4/13/2015
Date Closed:
Date of Initial DBCT Review: N/A
VA-NSOC Incident Number: VANSOC0619491
Date US-CERT Notified: 4/13/2015
US-CERT Case Number: INC000000458967
US-CERT Category: Category 6 - Investigation
No. of Credit Monitoring:
No. of Loss Notifications: 61

Incident Summary

On 03/19/15, 03/26/15, and 04/02/15, 61 potential research study participants were sent letters with incorrect addresses on three different occasions. Two participants contacted the facility to say that they received letters that included their address, but another person's name instead of theirs. Because the contact database contained information from Veterans who participated in research years ago, staff assumed that this meant that the addresses in that contact database were no longer valid. However, on the morning of 04/13/15, the primary investigator (PI), regulatory coordinator, and study coordinator reviewed the problem. They cross checked the contact database with the mail out recipient list and discovered that the list had been sorted incorrectly, which resulted in up to 61 instances of Veteran A receiving Veteran B's recruitment letter. The recruitment letter(s) indicate that the study being recruited for is a "PTSD and Smoking Cessation" study.

Incident Update

04/14/15:

The Incident Resolution Service Team has determined that sixty-one (61) Veterans will be sent a HIPAA notification letter.

Resolution

The study team will conduct 50% checks of mail merges (verifying address matched to Veteran name). If any discrepancies are found, a 100% verification process will be used..

DBCT Decision Date:

DBCT

No DBCT decision required. This has been left on the report since it affected more than 50 individuals.

Security Privacy Ticket Number: PSETS0000118257

DBCT Category: Mishandling

Organization: VISN 22
Long Beach, CA

Date Opened: 4/16/2015

Date Closed:

Date of Initial DBCT Review: 4/21/2015

VA-NSOC Incident Number: VANSOC0619729

Date US-CERT Notified: 4/16/2015

US-CERT Case Number: INC000000460111

US-CERT Category: Category 6 - Investigation

No. of Credit Monitoring: 138

No. of Loss Notifications: 91

Incident Summary

While disposing trash, a Veteran noticed files in a dumpster on campus. The Veteran retrieved the files and discovered they contained PII (i.e. SSN, date of birth, and home address). The files were dated 2007 through 2011, and appear to have originated from the Patient Business Office.

Incident Update

04/20/18:

It is estimated that the documents contained information on approximately 300 Veterans. VA Police were notified by the Veteran and subsequently took control of the files to log-in as evidence. The Privacy Officer was notified about the incident. The Veteran who discovered the files made a post on his personal Facebook page, referencing the incident and his post has been shared widely and commented on. In addition three related posts are on the VA Long Beach Healthcare System (VALBHS) Facebook page. VALBHS has addressed social medial posts, and included a message on their own page.

It appears that the accounts receivable office was moved to another facility. When employees moved out of their office, it is believed they left the documents behind. Contractors were hired to move the office furniture and found the documents and did not dispose of them properly. All the documents were accounts receivable related.

04/22/15:

The VA Police have completed an inventory of the documents recovered. There were a total of 358 documents and each one contained the Veterans SSN. There is no way to determine if any documents are not accounted for. It has further been verified that 77 of the Veterans are deceased. 229 Veterans will be offered credit protection services and 77 letters will be sent to their next of kin.

DBCT Decision Date:

DBCT

Based on the VA Data Breach criteria, this incident met the criteria for a breach, requiring each Veteran involved receive credit protection services or next of kin notification. The DBCT was briefed on this incident due to total number of affected Veterans.

Security Privacy Ticket Number: PSETS0000118459
DBCT Category: Mishandling
Organization: VISN 11
Battle Creek, MI
Date Opened: 4/22/2015
Date Closed: 4/24/2015
Date of Initial DBCT Review: N/A
VA-NSOC Incident Number: VANSOC0619929
Date US-CERT Notified: 4/22/2015
US-CERT Case Number: INC000000461576
US-CERT Category: Category 6 - Investigation
No. of Credit Monitoring: 37
No. of Loss Notifications:

Incident Summary

At 8:55 AM on 04/22/15, the Privacy Officer (PO) was notified by the Alternate PO that the Eye Clinic called stating that a Veteran had left with the Eye Clinic appointment list with his paperwork. The clinician realized what happened immediately and tried to find the Veteran, however, they were unable to. The list had the information of thirty seven (37) Veterans consisting of, names, full SSNs, co pay status, service connection rating, and telephone numbers.

Incident Update

04/22/15:

The Incident Resolution Service Team has determined that 37 Veterans will be sent letters offering credit protection services.

Resolution

The Clinicians in the Eye Clinic were educated on 04/22/15 to keep appointment lists concealed within a folder to distinguish between their work and paperwork of the Veterans. In addition, the clinicians were advised to ensure that they are giving the correct information to Veterans, to prevent such incidents from happening in the future. The Privacy Officer sent a self-addressed, stamped envelope to the Veteran to retrieve the information on 04/22/15.

DBCT Decision Date:**DBCT**

No DBCT decision is required. This is informational for Mishandling incidents and is the representative ticket. There were a total of 112 Mishandling incidents this reporting period. Because of repetition, the other 111 are not included in this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Security Privacy Ticket Number: PSETS0000118572
DBCT Category: Mismailed
Organization: VACO Field Program Office
Atlanta, GA
Date Opened: 4/23/2015
Date Closed:
Date of Initial DBCT Review: N/A
VA-NSOC Incident Number: VANSOC0620034
Date US-CERT Notified: 4/23/2015
US-CERT Case Number: INC000000462189
US-CERT Category: Category 6 - Investigation
No. of Credit Monitoring:
No. of Loss Notifications: 1

Incident Summary

A Veteran brought in a copy of a letter he received from the Health Eligibility Center (HEC) that belonged to another individual.

Incident Update

04/24/15:
The Incident Resolution Service Team has determined that the Veteran whose information was disclosed will be sent a notification letter.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for Mismatched incidents and is the representative ticket. There were a total of 204 Mismatched incidents this reporting period. Because of repetition, the other 203 are not included in this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Security Privacy Ticket Number: PSETS0000118630

DBCT Category: Mishandling

Organization: VISN 08
Bay Pines, FL

Date Opened: 4/27/2015

Date Closed:

Date of Initial DBCT Review: 5/5/2015

VA-NSOC Incident Number: VANSOC0620098

Date US-CERT Notified: 4/27/2015

US-CERT Case Number: INC000000463141

US-CERT Category: Category 6 - Investigation

No. of Credit Monitoring: 60

No. of Loss Notifications:

Incident Summary

On 04/24/15, a Business Office Service (BOS) employee reported that 64 Veteran authorizations for December were unable to be found. The BOS is conducting a search to locate the documents.

Incident Update

05/04/15:

The Privacy Officer reported that two authorizations were found and accounted for. The BOS is continuing to search for the remaining 62 authorizations.

05/12/15:

Two more authorization has been found, which leave 60 unaccounted for.

05/12/15:

The Incident Resolution Service Team has determined that sixty Veterans will be sent letters offering credit protection services.

DBCT Decision Date: 05/12/2015

DBCT

DBCT agreed that Credit Protection Services should be offered to the affected Veterans.