

Information Security Monthly Activity Report*

February 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)
4,357,398



Malware (Blocked/Contained)
930,583,011



Suspicious/Malicious Emails (Blocked)
68,326,883



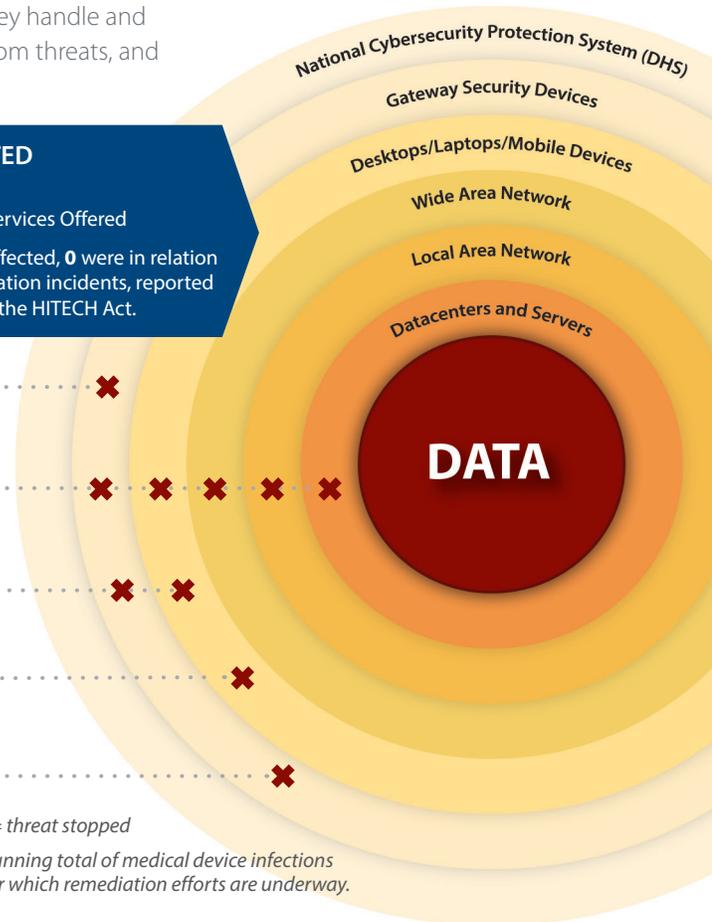
Infected Medical Devices (Contained)**
9



Outgoing Unencrypted Emails
76 Associated Privacy/Security Events
16,690 Total Emails Blocked

✘ = threat stopped

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



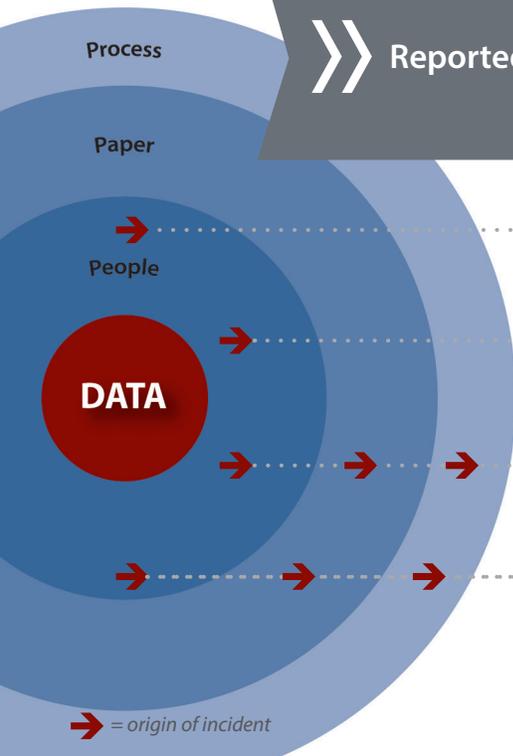
Reported Events



891 VETERANS AFFECTED

- 705 Notifications
- 186 Credit Protection Services Offered

Of the total # of Veterans affected, **770** were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



Lost and Stolen Device Incidents
36



Lost PIV Cards
140



Mishandled Incidents
118



Mis-mailed Incidents
136 Paper Mis-mailings

6 Pharmacy-item Mis-mailings
out of **6,537,156** 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
February 1-28, 2015

Security Privacy Ticket Number: PSETS0000114698
Incident Type: Mishandled/ Misused Physical or Verbal Information
Organization: VISN 09
Nashville, TN
Date Opened: 2/2/2015
Date Closed: 2/6/2015
Date of Initial DBCT Review: N/A
VA-NSOC Incident Number: VANSOC0616334
Date US-CERT Notified: 2/2/2015
US-CERT Case Number: INC000000438256
US-CERT Category: Category 6 - Investigation
No. of Credit Monitoring:
No. of Loss Notifications: 1
DBCT Category: Mismatched

Incident Summary

Veteran B notified the Privacy Officer of a travel claim form that was sent to him in error. It was determined that when the VA Travel Office was attempting to mail a claim for reimbursement of travel expenses to Veteran A, they inadvertently mailed that form along with a Travel Letter to Veteran B. Information on the travel claim form belonging to Veteran A included his full name, last four of his SSN, and home address.

Incident Update

02/02/15:

The Incident Resolution Service Team has determined that Veteran A will be sent a general notification letter.

Resolution

Documents that were mis-mailed were returned to the Privacy Officer. The issue has been referred to the Chief, Business Office for action. The employee involved with this incident has been educated and reminded to always perform a quality check of any documents being mailed to a Veteran.

DBCT Decision Date:**DBCT**

No DBCT decision is required. This is informational for Mis-Mailed incidents and is the representative ticket. There were a total of 136 Mis-Mailed incidents this reporting period. Because of repetition, the other 135 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: PSETS0000114754
Incident Type: Mishandled/ Misused Physical or Verbal Information
Organization: VISN 23
Minneapolis, MN
Date Opened: 2/3/2015
Date Closed: 2/6/2015
Date of Initial DBCT Review: N/A
VA-NSOC Incident Number: VANSOC0616406
Date US-CERT Notified: 2/3/2015
US-CERT Case Number: INC000000438606
US-CERT Category: Category 6 - Investigation
No. of Credit Monitoring:
No. of Loss Notifications: 1
DBCT Category: Mishandling

Incident Summary

Veteran A was provided Veteran B's medication.

Incident Update

02/03/15:

The Incident Resolution Service Team has determined that Veteran B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

The Pharmacy supervisor provided QA training to technicians.

DBCT Decision Date:**DBCT**

No DBCT decision is required. This is informational for Mis-Handling incidents and is the representative ticket. There were a total of 118 Mis-Handling incidents this reporting period. Because of repetition, the other 117 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: PSETS0000114825
Incident Type: Mishandled/ Misused Physical or Verbal Information
Organization: VHA CMOP
Hines, IL
Date Opened: 2/4/2015
Date Closed: 2/17/2015
Date of Initial DBCT Review: N/A
VA-NSOC Incident Number: VANSOC0616478
Date US-CERT Notified: 2/4/2015
US-CERT Case Number: INC000000439088
US-CERT Category: Category 6 - Investigation
No. of Credit Monitoring:
No. of Loss Notifications: 1
DBCT Category: CMOP Mismatched

Incident Summary

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. The Great Lakes 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.

Incident Update

02/04/15:

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

Resolution

On 2/4/15, the CMOP employee was counseled and retrained in proper packing procedures.

DBCT Decision Date:**DBCT**

No DBCT decision is required. This is informational for Mis-Mailed CMOP incidents and is the representative ticket. There were a total of six Mis-Mailed CMOP incidents out of 6,537,156 total packages (9,268,009 total prescriptions) mailed out for this reporting period. Because of repetition, the other five are not included in this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number: PSETS0000114867
Incident Type: Missing/Stolen Equipment
Organization: VISN 04
Altoona, PA
Date Opened: 2/4/2015
Date Closed: 2/20/2015
Date of Initial DBCT Review: N/A
VA-NSOC Incident Number: VANSOC0616520
Date US-CERT Notified: 2/4/2015
US-CERT Case Number: INC000000439185
US-CERT Category: Category 1 - Unauthorized Access
No. of Credit Monitoring:
No. of Loss Notifications:
DBCT Category: Unencrypted Desktop Missing

Incident Summary

A desktop PC which was located in the boiler plant, was unaccounted for during an inventory by logistics. The last time it was inventoried was on 02/27/14. It was in a locked cage area.

Incident Update

02/09/15:

The workstation was used to monitor boiler plant controls and does not store any VA sensitive information.

Resolution

The Service Chief informed the Information Security Officer (ISO) that the missing computer was not a networked device but was purchased as a backup computer for the boiler control system. There were two PC's which no one could ever get to work as intended as boiler control computers. One was turned in to Information Resource Management (IRM) since it was not capable of being used for its intended purpose and the one in question became missing sometime during the past year. No one could remember seeing two computers but they do remember the one which was still in a cardboard box sitting on the grate. That one was the one turned in to IRM. If the computer in question had been in service, it would have been known immediately that it had been removed. The Service Chief will follow up with all the boiler plant personnel for any further details. The ISO uploaded the official completed Report-of-survey.

DBCT Decision Date:**DBCT**

No DBCT decision was required. This was left on the report as it is missing unencrypted equipment.

Security Privacy Ticket Number: PSETS0000114926
Incident Type: Mishandled/ Misused Physical or Verbal Information
Organization: VISN 19
Denver, CO
Date Opened: 2/5/2015
Date Closed:
Date of Initial DBCT Review: 2/10/2015
VA-NSOC Incident Number: VANSOC0616576
Date US-CERT Notified: 2/5/2015
US-CERT Case Number: INC000000439546
US-CERT Category: Category 4- Improper Usage
No. of Credit Monitoring:
No. of Loss Notifications: 507
DBCT Category: Mishandling

Incident Summary

A former VA employee, released a wait list to a reporter as a "whistle blower." The list had scheduled dates, last four digits of the SSN, and clinic names. It is possible the list also had first and last name. The media used the list in reporting a story and had stated "they have redacted protected health information (PHI)" to protect the Veterans. However, it is unknown when and who redacted the information and how many unredacted lists could still be at large. This incident occurred in the Sleep Clinic, a clinic which previously had two missing laptops this year. It is unknown if this is related, but it is possible.

Incident Update

02/17/15:

The list contains information on 508 patients. It is not known how the employee obtained the list.

02/25/15:

The facility privacy officer has provided the list which the media obtained. At this point, it is not known how the media obtained the list and when it was redacted. The employee left employment on 6/27/14 and contacted the media in September, 2014. The employee's computer access has been terminated. It is not known if the employee printed the list prior to separating or if a current employee provided them the list. The DBCT suggested that the VISN Public Affairs Officer (PAO) contact the media to ask for the original document to be returned to the VA. The VISN PAO has stated that relations between the facility and the local media are not the best and there have been several negative stories about the facility in the news recently. It is possible the list was redacted prior to leaving VA custody.

03/02/15:

The Regional Office of Public and Intergovernmental Affairs (OPIA) has consulted with the facility and reports that the individual has admitted to taking VA records, lists and emails with them.

03/09/15:

The documents in the HAS shared folder were reviewed. These are the documents which the employee had access to. The document contains the Veterans name, last initial/last four of social, the patient's desired date, and the referring clinic. There was one duplicate name on the list so it is 507 total patients affected.

DBCT Decision Date: 03/10/2015

DBCT

The Data Breach Core Team determined that a breach did occur. All 507 Veterans will be sent a HIPAA notification letter. This is a HITECH reportable breach and a press release will be done.

Security Privacy Ticket Number: PSETS0000115095
Incident Type: Unauthorized Physical or Verbal Access
Organization: VISN 21
San Francisco, CA
Date Opened: 2/9/2015
Date Closed:
Date of Initial DBCT Review: 2/24/2015
VA-NSOC Incident Number: VANSOC0616873
Date US-CERT Notified: 2/9/2015
US-CERT Case Number: INC000000440817
US-CERT Category: Category 6 - Investigation
No. of Credit Monitoring: 270
No. of Loss Notifications:
DBCT Category: Mishandling

Incident Summary

The Privacy office was notified that a clinic in module 1 was broken into over the past weekend. A VA employee found bed sheets, gowns, toothbrushes, and office supplies scattered throughout the room. In addition to the exam room, the intruder pried open locks at the clerical station in Module 1. Encounter forms and patient information were scattered throughout the desk area. It has not been determined if patient information was at risk. Several medication carts in the exam room were opened and needles, syringes, medications, scalpels, and a long list of medical items were noted as missing.

Incident Update

02/11/15:

The clinical supervisor determined there was approximately 250 encounters potentially exposed.

03/10/15:

The Data Breach Core Team has determined that 20 Veterans will be sent letters offering credit protection services and 250 will receive HIPAA notification letters.

DBCT Decision Date: 03/10/2015

DBCT

03/10/15:

The DBCT determined that due to the theft of medical supplies there is no guarantee that the PHI/PII was not also at risk. Therefore this is considered a data breach and notification and/or credit protection services will be offered.

Security Privacy Ticket Number: PSETS0000115629
Incident Type: Missing/Stolen Equipment
Organization: VISN 17
Temple, TX
Date Opened: 2/19/2015
Date Closed: 2/23/2015
Date of Initial DBCT Review: N/A
VA-NSOC Incident Number: VANSOC0617243
Date US-CERT Notified: 2/19/2015
US-CERT Case Number: INC000000443559
US-CERT Category: Category 1 - Unauthorized Access
No. of Credit Monitoring:
No. of Loss Notifications:
DBCT Category: Unencrypted Desktop Missing

Incident Summary

A Psychology employee notified the Information Security Officer (ISO) that while conducting inventory, it was discovered that a computer under Psychology's Equipment Inventory Listing is unaccounted for. A search to find the computer used by Psychology for relaxation therapy was conducted however; the computer was not physically located. Logistics and Information Technology (IT) do not have paperwork documenting the computer was turned in and the hard drive was sanitized. The computer was never connected to the VA network. First initial and last four were stored on the PC to use with biofeedback therapy but no other sensitive information was stored.

Incident Update

02/23/15:

The Incident Resolution Service Team has determined that no data breach has occurred. This system does not process, store, or transmit VA sensitive data. A Report of Survey and VA police report are pending. VA Police have initiated an investigative report regarding this missing equipment. Staff continue to search for the device and will immediately contact the ISO and VA Police if found. The ISO will update this ticket if the device is found.

Resolution

Psychology Service is now performing inventory audits on a quarterly basis and is identifying if other biofeedback therapy systems are being used by staff and if not those systems will be turned in immediately to logistics and hard drive sanitization will be performed by IT. This system was never on the VA network.

DBCT Decision Date:

DBCT

No DBCT decision was required. This was left on the report as it is missing unencrypted equipment.