

Information Security Monthly Activity Report*



November 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) x
178,901,774



Malware (Blocked/Contained) x x x x x
621,526,267



Suspicious/Malicious Emails (Blocked) x x
85,614,081



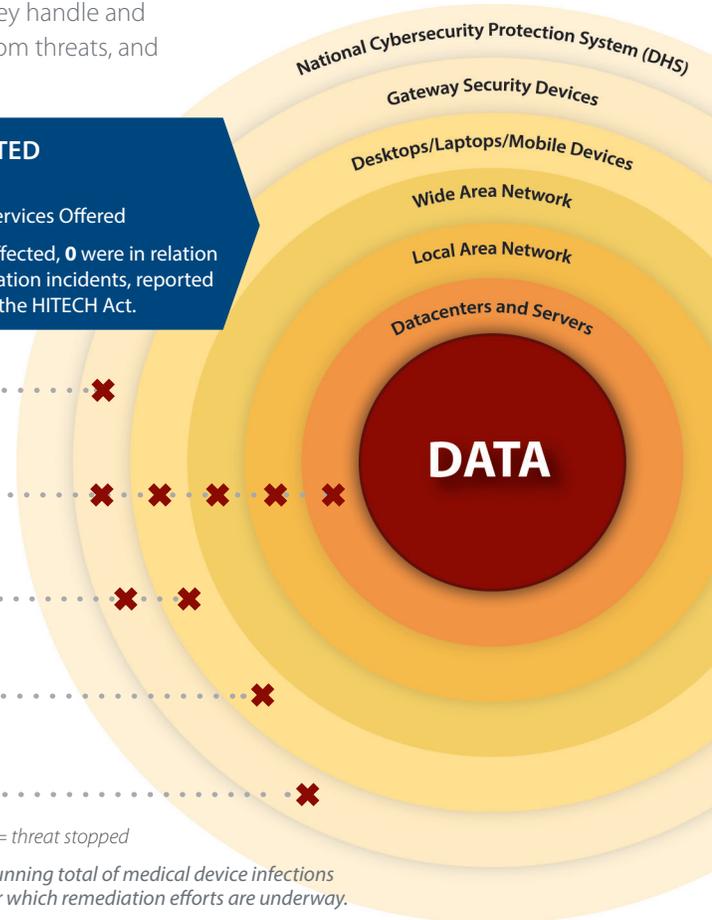
Infected Medical Devices (Contained)** x
0



Outgoing Unencrypted Emails x
61 Associated Privacy/Security Events
12,939 Total Emails Blocked

x = threat stopped

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



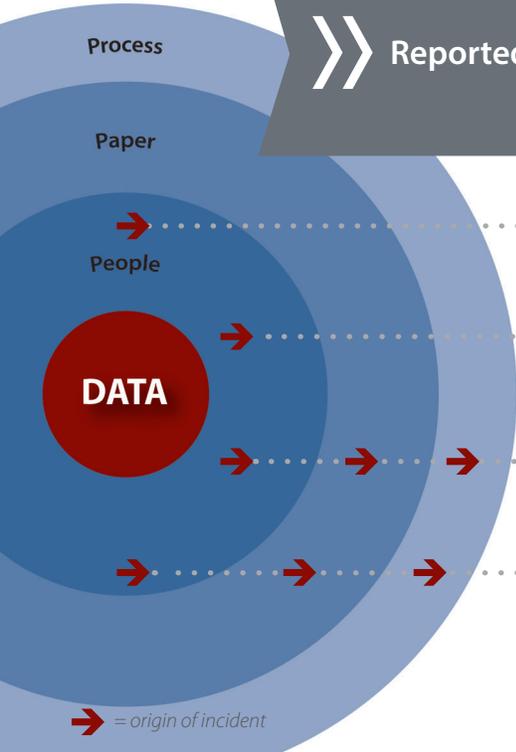
Reported Events



693 VETERANS AFFECTED

- 134 Notifications
- 559 Credit Protection Services Offered

Of the total # of Veterans affected, 616 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
156



Mishandled Incidents
64



Mis-mailed Incidents
114 Paper Mis-mailings

1 Pharmacy-item Mis-mailings
 out of **6,145,859** 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
Data Breach Response Service

Monthly Report to Congress on Data Incidents

November 1 - 30, 2015

Security Privacy Ticket Number: PSETS0000126684

DBCT Category: CMOP Mismatched

Organization: VHA CMOP
Leavenworth, KS

Date Opened: 11/2/2015

Date Closed:

Date of Initial DBCT Review: 11/10/2015

No. of Credit Monitoring:

No. of Loss Notifications: 2

Incident Summary

Patient A received a Medline Industries medical supply and paperwork intended for Patient B. Patient B received a Medline Industries medical supply and paperwork intended for Patient A. Patient A and Patient B's name and type of medical supply was compromised. Patient A reported the incident to Meds By Mail (site 741) and a replacement has been requested for Patient B. Patient B reported the incident to Leavenworth, KS Consolidated Mail Outpatient Pharmacy (CMOP site 760) and a replacement has been requested for Patient A. Leavenworth CMOP investigation concludes that this was a Medline packing error. The packing errors have been reported to Medline for investigation and corrective action.

Total number of affected Patients: 2

Incident Update

11/02/15:

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

DBCT Decision Date: 11/10/2015

DBCT No DBCT decision is required. This is informational for Mis-Mailed CMOP incidents and is the representative ticket. There was only 1 Mis-Mailed CMOP incident out of 6,145,859 total packages (9,153,784 total prescriptions) mailed out for this reporting period. In this incident, the affected individuals will receive HIPAA notification letters.

Security Privacy Ticket Number: PSETS0000126695

DBCT Category: Mismailed

Organization: VBA
St Paul, MN

Date Opened: 11/2/2015

Date Closed: 11/5/2015

Date of Initial DBCT Review: 11/10/2015

No. of Credit Monitoring: 1

No. of Loss Notifications:

Incident Summary

Veteran A received a letter that contained a rating decision belonging to Veteran B.

Incident Update

11/02/15:

The Incident Resolution Service Team has determined that Veteran B will be sent a letter offering credit protection services.

Resolution

The Supervisor provided awareness training to responsible employee on 11/03/15 on the importance of reviewing outgoing mail for PII belonging to other claimants.

DBCT Decision Date: 11/10/2015

DBCT No DBCT decision is required. This is informational for Mis-Mailed incidents and is the representative ticket. There were a total of 114 Mis-Mailed incidents this reporting period. Because of repetition, the other 113 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: PSETS0000126875

DBCT Category: Mishandling

Organization: VISN 01
Boston, MA

Date Opened: 11/5/2015

Date Closed: 12/2/2015

Date of Initial DBCT Review: 11/10/2015

No. of Credit Monitoring: 259

No. of Loss Notifications:

Incident Summary

A clinic list was found in a public bathroom in a heavily trafficked area. The list was printed on November 4th, 2015. Some names are duplicates but all include full SSN and procedure information.

Incident Update

11/06/15:

After investigation and cross referencing names on the list, the initial count is 285 affected individuals. Despite the list being printed on November 4th and being found on November 5th, it is not likely that it was left overnight, however it is unable to be determined exactly how long it was exposed for. After talking to the Privacy Officer (PO), it was determined that the list is an 11 page clinic list that covered the entire month of October. The document was found in a public area restroom in a heavily trafficked area that is across from the current cafeteria and around the corner from the Veterans Canteen Store. Housekeeping does maintain the restroom frequently that is why it is not believed that it was left overnight. There are no cameras in the area that would have captured the entrance so it is unable to be determined whom/how many people would have gone in the restroom. The document has since been retrieved.

11/10/15:

The Data Breach Core Team has determined that 285 Veterans will be sent letters offering credit protection services.

12/2/2015:

After further review of the information and removal of duplicate names, the final count of affected individuals is 259.

Security Privacy Ticket Number: PSETS0000126875 (continued)

Resolution

The document was retrieved. Education regarding the proper handling of information will be provided to service at their next staff meeting.

DBCT Decision Date: 11/10/2015

DBCT The Data Breach Core Team has determined that 285 Veterans will be sent letters offering credit protection services.

Security Privacy Ticket Number: PSETS0000127395
DBCT Category: Mishandling
Organization: VISN 22
Loma Linda, CA

Date Opened: 11/18/2015

Date Closed: 12/9/2015

Date of Initial DBCT Review: 11/24/2015

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

Veteran A was given Veteran B's discharge papers instead of his own.

Incident Update

11/19/15:
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 redacted notification letter has been attached to the incident ticket. The Privacy officer spoke to Veteran A who will shred the document. The Resident who caused the disclosure has completed both Talent Management System courses 10203 (Privacy and HIPAA Training) and 10176 (Privacy and Information Security Awareness Training).

DBCT Decision Date: 11/24/2015

DBCT No DBCT decision is required. This is informational for Mis-Handling incidents and is the representative ticket. There were a total of 64 Mis-Handling incidents this reporting period. Because of repetition, the other 63 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: PSETS0000127419

DBCT Category: Mishandling

Organization: VISN 08
Miami, FL

Date Opened: 11/19/2015

Date Closed:

Date of Initial DBCT Review: 11/24/2015

No. of Credit Monitoring: 126

No. of Loss Notifications:

Incident Summary

A nurse who was working on a project to convert ICD-9 diagnoses to ICD-10 lost a list of names and SSNs of Veterans whose diagnoses were to be converted. Two pages of a three page report were lost in the VA Canteen. Each page contained the name and SSNs of 60 Veterans.

Incident Update

11/24/15:

The Incident Resolution Service Team has determined that 120 Veterans will be sent letters offering credit protection services.

11/25/15:

Update: Per the Privacy Officer, the count is 126.

DBCT Decision Date: 11/24/2015

DBCT No DBCT decision was required. Based on the VA Breach Criteria, all affected Veterans are to be offered Credit Protection Services. This incident was presented to the DBCT for awareness due to the number of Veterans affected.

Security Privacy Ticket Number: PSETS0000127470
DBCT Category: Encrypted Laptop Stolen
Organization: VBA
Washington, DC

Date Opened: 11/20/2015

Date Closed:

Date of Initial DBCT Review: 11/24/2015

No. of Credit Monitoring:

No. of Loss Notifications: 84

Incident Summary

A VA Contractor reported to the Contracting Officer's Representative (COR) that a personal laptop had been stolen. This personal laptop was used by Contractor to support VBA M Data Extraction (MDE) Contract medical exams.

Incident Update

11/20/15:

The COR for the contract states that the contractor, QTC, is going to provide credit monitoring for 84 individuals in this case. The physician states that he did not store PHI on the laptop, and QTC states that doing so is against policy, but they have no way of proving he did not, so they are calling it a data breach. The information that could have been stored was name, SSN, and diagnoses.

12/01/15:

The Information Security Officer (ISO) and Privacy Officer (PO) have completed their investigation and new information has been provided to them. Full SSN would not have been on the laptop, only name, QTC identification number, and medical information. The contract states that VA will provide notification if needed.

DBCT Decision Date: 11/24/2015

DBCT After new information was provided, it was determined this was a VA data breach, as information on the laptop included names and medical information of 84 Veterans. VA will provide notification to the 84 Veterans involved.

Security Privacy Ticket Number: PSETS0000127473
DBCT Category: IT Equipment Inventory
Organization: VISN 12
Madison, WI

Date Opened: 11/20/2015

Date Closed: 12/7/2015

Date of Initial DBCT Review: 11/24/2015

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

A Report of Survey (ROS) indicated 8 computers were not located during last inventory. All have encrypted hard drives.

Incident Update

11/20/15:
The Incident Resolution Service Team has determined that there was an IT equipment inventory issue. No data breach has occurred, as all devices were encrypted.

Resolution

The Report of Survey indicated 8 computers were not located during last inventory. All have encrypted hard drives.

DBCT Decision Date: 11/24/2015

DBCT This incident was briefed to the DBCT, but no DBCT decision is required. This is informational for IT Equipment Inventory incidents and is the representative ticket. There were four (4) IT Equipment Inventory Incidents this reporting period.