

Information Security Monthly Activity Report*



December 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)
181,188,372



Malware (Blocked/Contained)
546,969,366



Suspicious/Malicious Emails (Blocked)
100,778,911



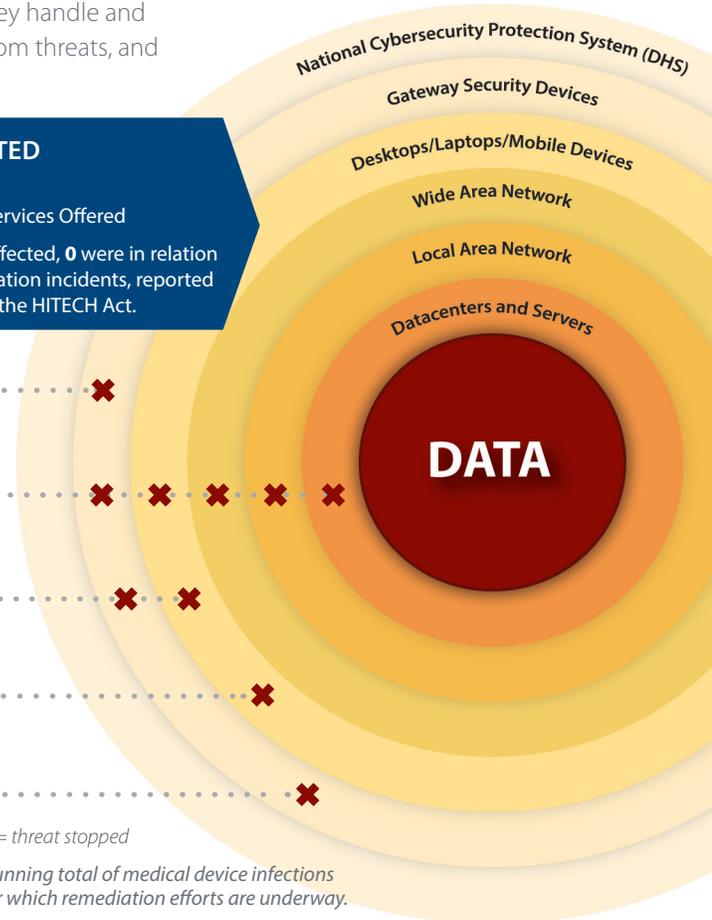
Infected Medical Devices (Contained)**
0



Outgoing Unencrypted Emails
67 Associated Privacy/Security Events
9,801 Total Emails Blocked

✘ = threat stopped

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



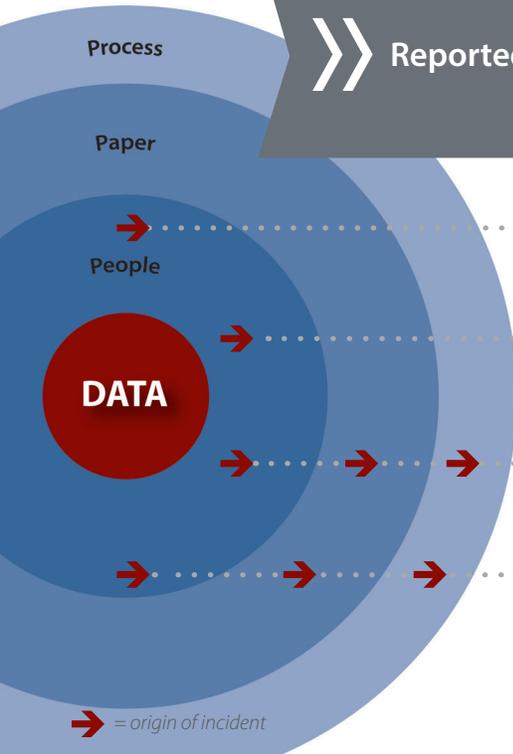
Reported Events



394 VETERANS AFFECTED

- 181 Notifications
- 213 Credit Protection Services Offered

Of the total # of Veterans affected, **240** 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
131



Mishandled Incidents
78



Mis-mailed Incidents
169 Paper Mis-mailings

3 Pharmacy-item Mis-mailings
out of **6,991,142** Total Mailings

*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.

→ = origin of incident

DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Data Breach Response Service

Monthly Report to Congress of Data Incidents
December 1-31, 2015

Security Privacy Ticket Number: PSETS0000128089
DBCT Category: IT Equipment Inventory
Organization: VACO OI&T
Washington, DC

Date Opened: 12/3/2015

Date Closed:

Date of Initial DBCT Review: 12/15/2015

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

It was reported that items included on a submitted Report of Survey (ROS) were unable to be located during the end of the November 2015 inventory.

Incident Update

12/07/15:

After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that no incident has occurred and therefore there is no loss of VA information or data as all noted items of concern were encrypted.

DBCT Decision Date: 12/15/2015

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 representative ticket. There were a total of three IT Equipment Inventory Incidents this reporting period. Because of repetition, the other two are not included in this report.

Security Privacy Ticket Number: PSETS0000128165
DBCT Category: Mismailed
Organization: VISN 19
Grand Junction, CO

Date Opened: 12/4/2015
Date Closed: 12/17/2015
Date of Initial DBCT Review: N/A
No. of Credit Monitoring:
No. of Loss Notifications: 1

Incident Summary

The Privacy Officer (PO) received a complaint from Veteran A indicating that he had received a letter containing lab results intended for Veteran B included in correspondence he received from his Primary Care Provider. The PO spoke with Veteran A and requested that the letter be returned to the local VA clinic to which agreed.

Incident Update

12/07/15:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that Veteran B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

Medical administrative staff member have received remedial training to ensure proper procedures are adhered to.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for Mismailed incidents and is the representative ticket. There were a total of 169 Mismailed incidents this reporting period. Because of repetition, the other 168 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: PSETS0000128199

DBCT Category: CMOP Mismatched

Organization: VHA CMOP
Tucson, AZ

Date Opened: 12/7/2015

Date Closed:

Date of Initial DBCT Review:
N/A

No. of Credit Monitoring:

No. of Loss Notifications: 1

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 North Texas Medical Center and a replacement has been requested for Patient B. Tucson Consolidated Mail Outpatient Pharmacy (CMOP) investigation concluded that this was a CMOP packing error. The CMOP employee will be counseled and retrained in proper packing procedures.

Incident Update

12/07/15:

After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that Veteran B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for Mismatched CMOP incidents and is the representative ticket. There were a total of three Mismatched CMOP incidents out of 6,991,142 total packages (10,284,549 total prescriptions) mailed out for this reporting period. Because of repetition, the other two are not included in this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number: PSETS0000128229

DBCT Category: Mishandling

Organization: VISN 20
Seattle, WA

Date Opened: 12/7/2015

Date Closed: 1/8/2016

Date of Initial DBCT Review: 12/15/2015

No. of Credit Monitoring: 58

No. of Loss Notifications:

Incident Summary

On December 7, 2015 a housekeeping employee reported to the Seattle Privacy Officer (PO) that documents containing the full name and Social Security Number of 55 patients/Veterans and a copy of an EKG report containing the full name, Social Security Number, date of birth and the EKG date were left unsecured at the "old ICU" front desk. The Seattle PO responded and took possession of the documents.

Incident Update

12/15/15:

After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Core Team determined that 58 Veterans will be sent letters offering credit protection services.

Resolution

The investigation failed to identify who might have been at fault for leaving the documents unsecured. All service line members are aware of the incident and encouraged to pay better attention when disposing of documents containing PII.

DBCT Decision Date: 12/15/2015

DBCT

The DBCT determined that there was more than a low risk of compromise and that the 58 affected individuals would be sent letters offering credit protection services.

Security Privacy Ticket Number: PSETS0000128573

DBCT Category: Mishandling

Organization: VISN 01
Manchester, NH

Date Opened: 12/15/2015

Date Closed:

Date of Initial DBCT Review: N/A

No. of Credit Monitoring: 1

No. of Loss Notifications:

Incident Summary

A Prosthetic employee accidentally sent a consult to Veteran A with Veteran B's information. Veteran A's wife brought the information to the supervisor to be reported to the Privacy Officer (PO).

Incident Update

12/15/15:

After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that Veteran B will be sent a letter offering credit protection services.

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 78 Mishandling incidents this reporting period. Because of repetition, the other 77 are not included in this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.