Information Security
Monthly Activity Report*

INFOCON LEVEL
CRITICAL
SEVERE
ELEVATED
GUARDED
NORMAL

January 2016

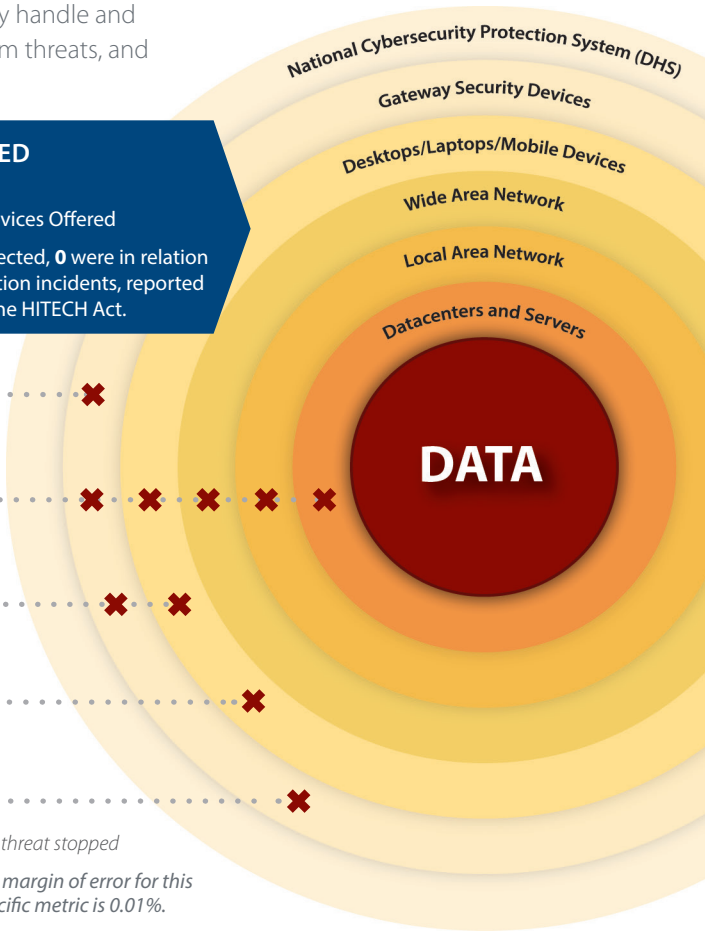
VA uses a defense-in-depth approach to information security to protect the data we hold on Veterans. While the defense-in-depth approach protects from inbound threats and contains other data exposing incidents, VA relies on employees to protect Veteran information they handle and transmit. This graphic 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)**
76,509,609

Malware (Blocked/Contained)
638,306,982

Suspicious/Malicious Emails (Blocked)
99,260,056

Infected Medical Devices (Contained)
3

Outgoing Unencrypted Emails
94 Associated Privacy/Security Events
28,361 Total Emails Blocked

✖ = *threat stopped*

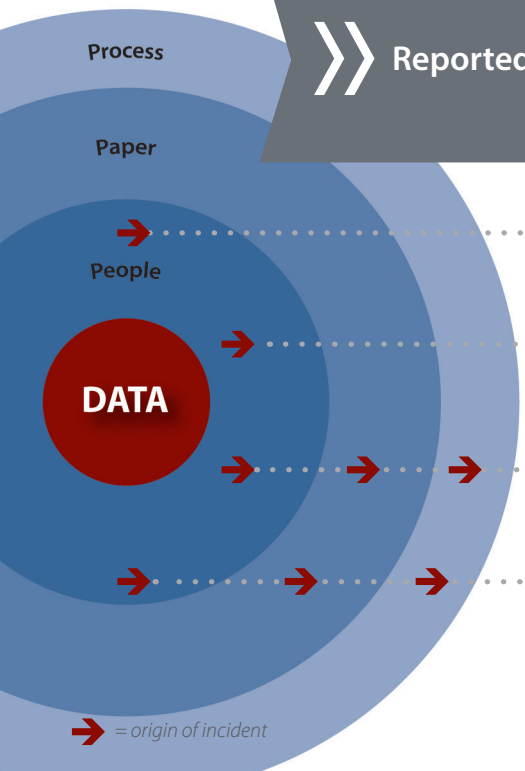
***The margin of error for this specific metric is 0.01%.*

Reported Events

568 VETERANS AFFECTED

- **271** Notifications
- **297** Credit Protection Services Offered

Of the total # of Veterans affected, **236** were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



Lost and Stolen Device Incidents
46

Lost PIV Cards
154

Mishandled Incidents
121

Mis-mailed Incidents
141 Paper Mis-mailings
10 Pharmacy-item Mis-mailings
out of **6,417,897** 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.

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

Monthly Report to Congress of Data Incidents

January 1-31, 2016

Security Privacy Ticket Number: PSETS0000129174

DBCT Category: Mishandling

Organization: VISN 11
Battle Creek, MI

Date Opened: 1/4/2016

Date Closed: 2/1/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

A clinical provider entered a Compensation and Pension examination performed on Veteran A into Veteran B's record in error. The Medical Records associated with the examination were then inappropriately released to Veteran B. Veteran B discovered the error and returned the records to the Release of Information (ROI) Office.

Incident Update

01/04/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that Veteran A will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

The employee involved in this incident has been educated on the appropriate processes regarding ensuring Veteran information is entered into the correct chart.

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 121 mishandling incidents this reporting period. Because of repetition, the other 120 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: PSETS0000129533

DBCT Category: Mismailed

Organization: VISN 12
Hines, IL

Date Opened: 1/8/2016

Date Closed: 1/27/2016

Date of Initial DBCT Review: 1/19/2016

No. of Credit Monitoring:

No. of Loss Notifications: 84

Incident Summary

The secretary for Nutrition and Food Services mistakenly mailed Veterans' documents that contained the full name and address of other Veterans who are prescribed the same type medication. A Veteran called to report that he had received an envelope with other Veterans names and addresses, but he shredded the information.

Incident Update

01/11/16:
The information that was provided to the secretary inadvertently resulted in seven Veteran's receiving a combined total of 84 flyers that were intended for other Veterans. For example, Veteran A received his notice of the change plus a notice for 14 other Veterans in the same envelope. The information was to notify the Veterans that due to contract changes a new company would be providing the formulary for their prescription. Once the Service realized the error, they started contacting the Veterans to retrieve the documents. After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 84 Veterans will be sent notification letters.

Resolution

The staff member responsible has been counseled and re-educated on handling patient information.

DBCT Decision Date: 01/19/2016

DBCT

No DBCT decision was required, but this ticket was presented to the DBCT due to the number of affected individuals.

Security Privacy Ticket Number: PSETS0000130409

DBCT Category: IT Equipment Inventory

Organization: VISN 20
Anchorage, AK

Date Opened: 1/25/2016

Date Closed: 1/25/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

The facility Chief Information Officer submitted two Reports of Survey that identified three PCs were missing from their IT equipment inventory. The last inventory dates for the three devices were 12/16/14, 12/24/14, and 01/02/15. IT staff have made an exhaustive search for the devices with no success.

Incident Update

01/25/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, § C (Risk Assessment), Paragraph 1 (d), the Data Breach Response Service has determined that no breach has occurred. The desktops were encrypted. Therefore this incident has a low probability of a risk of compromise due to the risk having been properly mitigated through established controls.

Resolution

The desktops were encrypted.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for IT Equipment Inventory incidents and is the representative ticket. There were a total of two IT Equipment Inventory Incidents this reporting period. Because of repetition, the other one was not included in this report.

Security Privacy Ticket Number: PSETS0000130423

DBCT Category: Mishandling

Organization: VISN 12
Chicago, IL

Date Opened: 1/25/2016

Date Closed:

Date of Initial DBCT Review: N/A

No. of Credit Monitoring: 97

No. of Loss Notifications:

Incident Summary

It was reported that a Program Application Specialist (PAS) clerk was working on project documentation which included multiple Veterans' personal information when Veteran A visited the clerk's desk with a question/inquiry. The employee turned the Veteran documentation over so the information could not be viewed. While talking with the clerk, Veteran A placed his tablet/folder on top of the project documentation. The clerk assisted Veteran A with his inquiry. Upon Veteran A's departure, he inadvertently picked up the project documentation that the clerk was working on along with his tablet/folder. When the clerk noticed that Veteran project information was missing, the employee notified her management and they attempted unsuccessfully to locate Veteran A.

Incident Update

01/25/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 97 Veterans will be sent letters offering credit protection services.

DBCT Decision Date: 02/02/2016

DBCT

No DBCT decision was required, but this ticket was presented to the DBCT due to the number of affected individuals.

Security Privacy Ticket Number: PSETS0000130549

DBCT Category: Mismailed

Organization: VISN 11
Ann Arbor, MI

Date Opened: 1/27/2016

Date Closed: 1/29/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

Veteran A received the pre-op evaluation letter of Veteran B, as the envelope was incorrectly addressed to Veteran A.

Incident Update

01/27/16:
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

Veteran A was sent a postage paid, self-addressed envelope on 01/27/16, to return the information of Veteran B to the facility Privacy Officer. The supervisors of the areas that could have possibly sent out the information will educate the staff to ensure they are placing the correct Veteran's information in the correct envelope.

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 141 mismailed incidents this reporting period. Because of repetition, the other 140 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: PSETS0000130600

DBCT Category: CMOP Mismailed

Organization: VHA CMOP
Charleston, SC

Date Opened: 1/27/2016

Date Closed: 2/3/2016

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 Orlando VA Medical Center and a replacement has been requested for Patient B. The Charleston 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

01/27/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that Patient B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

On 1/27/2016, 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 ten Mismailed CMOP incidents out of 6,417,897 total packages (9,525,235 total prescriptions) mailed out for this reporting period. Because of repetition, the other nine are not included in this report. In all incidents, Veterans will receive a notification letter.