

Information Security Monthly Activity Report*



March 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) **74,486,427**



Malware (Blocked/Contained) **754,465,668**



Suspicious/Malicious Emails (Blocked) **95,787,466**

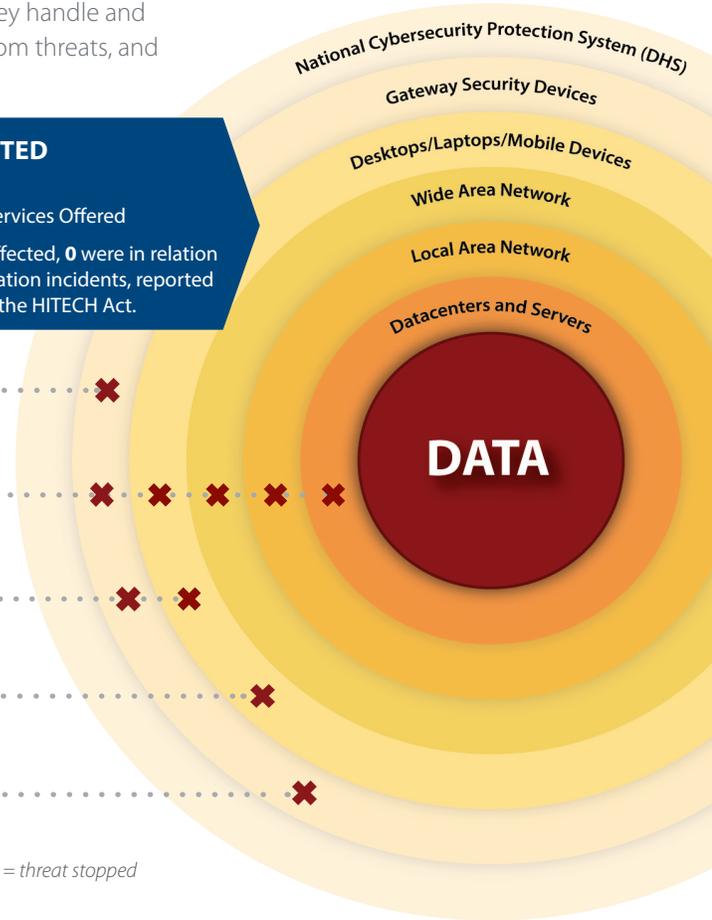


Infected Medical Devices (Contained) **0**



Outgoing Unencrypted Emails **88** Associated Privacy/Security Events
24,707 Total Emails Blocked

✗ = threat stopped



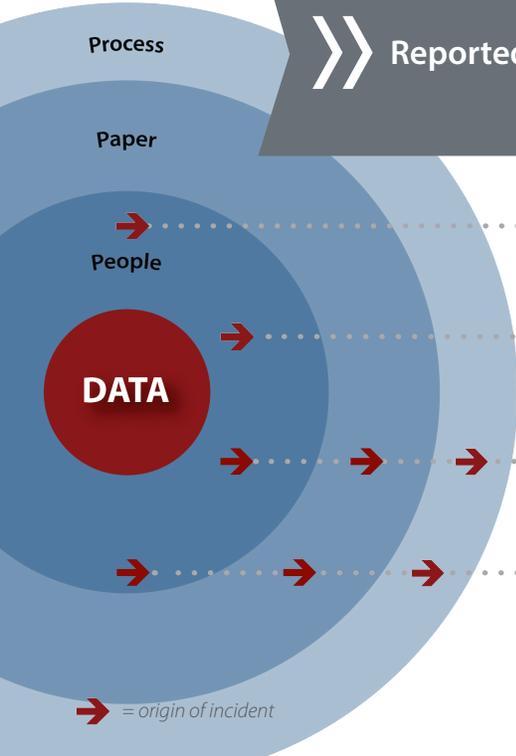
Reported Events



522 VETERANS AFFECTED

- 288 Notifications
- 234 Credit Protection Services Offered

Of the total # of Veterans affected, 417 were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



Lost and Stolen Device Incidents **54**



Lost PIV Cards **172**



Mishandled Incidents **89**



Mis-mailed Incidents **147**

3 Pharmacy-item Mis-mailings out of **7,121,160** 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 of Data Incidents
March 1 - 31, 2016

Security Privacy Ticket Number: PSETS0000132095

DBCT Category: Mismailed

Organization: VBA
St Louis, MO

Date Opened: 3/1/2016

Date Closed: 3/8/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring: 1

No. of Loss Notifications:

Incident Summary

Veteran A requested copies of his C-File but in the process of fulfilling the request, Veteran B's information was included in the response.

Incident Update

03/01/16:

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 letter offering credit protection services.

Resolution

Involved employee has been counseled and provided on-spot refresher training.

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 147 Mis-Mailed incidents this reporting period. Because of repetition, the other 146 are not included in this report, but are included in the "Mis-Mailed Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Security Privacy Ticket Number: PSETS0000132220
DBCT Category: Mishandling
Organization: VISN 20
Seattle, WA
Date Opened: 3/2/2016
Date Closed: 4/11/2016
Date of Initial DBCT Review: 3/8/2016
No. of Credit Monitoring: 70
No. of Loss Notifications: 141

Incident Summary

During the night of 02/28/16, a briefcase containing two lists of patient names were stolen from a physicians locked vehicle. The vehicle was parked in front of the employee's home where the car windows were shattered and the contents of the vehicle were stolen.

- The first list was generated for use at the VA Stand Down on 02/27/16.
- The lists identified 141 Veterans by first initial, last name, and last four digits of their Social Security Number.
- The information on the lists included the current status of Primary Care Service consults, and which Primary Care group the Veteran consults were assigned to.
- The lists did not include medical information or dates of birth.
- The second list was of patients in the provider's panel that are on opioids
- This lists identified 70 Veterans full name, full Social Security Number, date of birth, opioid prescription nomenclature, and last time ordered.
- No VA information technology resources were in the car at the time of the theft.
- The employee had completed training in the Talent Management System, Course #10176 (VA Privacy and Information Security Awareness and Rules of Behavior).
- Police Service, the Privacy Officer (PO), and the Information Security Officer (ISO) e were notified.

Incident Update

03/03/16:

After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 70 Veterans will be sent a letter offering credit protection services.

A HIPAA notification letter will be sent to 141 Veterans due to Protected Health Information (PHI) being disclosed.

Resolution

This has been referred to Senior VAPD leadership for mitigation and corrective action.

DBCT Decision Date:

DBCT

No DBCT decision needed. This is informational due to the number of Veterans affected.

Security Privacy Ticket Number: PSETS0000132361
DBCT Category: Mishandling
Organization: VISN 08
Gainesville, FL
Date Opened: 3/4/2016
Date Closed: 3/22/2016
Date of Initial DBCT Review: N/A
No. of Credit Monitoring: 1
No. of Loss Notifications:

Incident Summary

Veteran A received Veteran B's medication paperwork upon dispensing at the Pharmacy pick up window, but no medication. Veteran A was contacted by Pharmacy and agreed to return Veteran B's paperwork on 03/07/16 when his next appointment is.

Incident Update

03/04/16:
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

On March 4, 2016, pharmacy's dispensing procedures were not followed and this resulted in a privacy breach. Veteran A received Veteran B's medication information sheet. Upon researching pharmacy discovered that Veteran A's medication was in the bag but Veteran B's paperwork was in the same bag. When a pharmacist verifies a prescription (checks to ensure the correct medication is being dispensed and prints an address label sticker), they are to compare the medication to the patient's prescription paperwork before packaging medications and paperwork. In addition the dispensing pharmacist is to compare the patient's prescription paperwork to the patient's medication before dispensing to the patient. This comparison step of medication to paperwork was missed by both the checking pharmacist and dispensing pharmacist resulting in a breach of patient privacy. Pharmacy procedures have been reviewed by management staff to ensure each step provides for safe and confidential care. All pharmacy staff will be reminded of the procedures that must be followed in order to facilitate providing each and every veteran with the safest and most confidential care. In addition, the responsible checking pharmacist and dispensing pharmacist have been individually counseled on the importance of pharmacy procedures and how pertinent it is to follow these procedures to ensure our patients privacy and safety. They have both completed the required TMS training.

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 89 Mis-Handling incidents this reporting period. Because of repetition, the other 88 are not included in this report, but are included in the "Mis-Handling Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Security Privacy Ticket Number: PSETS0000132637
DBCT Category: IT Equipment Inventory
Organization: VBA
Washington, DC

Date Opened: 3/10/2016

Date Closed: 3/18/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

During an inventory of IT equipment, some printers, monitors, computers and BlackBerrys could not be located by Assets Management. Reports of Surveys have been uploaded to this ticket.

Incident Update

03/11/16:

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. All devices capable of holding any VA data (Laptop x3/Desktop x1) were encrypted. In addition any devices with cellular/wireless capabilities (Blackberry x4) will be/have been disabled per policy. Therefore this incident has a low probability of a risk of compromise due to the risk having been properly mitigated through established controls.

Resolution

Report of survey has been uploaded; Laptops and desktops had whole disk encryption.

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 6 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 5 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Security Privacy Ticket Number: PSETS0000132937
DBCT Category: CMOP Mismatched
Organization: VHA CMOP
Murfreesboro, TN
Date Opened: 3/17/2016
Date Closed: 3/23/2016
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 medical center and a replacement has been requested for Patient B. Murfreesboro 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

03/17/16:

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 3/17/2016, the CMOP employee was counseled and retrained in proper packing procedures

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for Mis-Mailed CMOP incidents and is the representative ticket. There were a total of 3 Mis-Mailed CMOP incidents out of 7,121,160 total packages (10,477,211 total prescriptions) mailed out for this reporting period. Because of repetition, the other 2 are not included in this report, but are included in the "Mis-Mailed CMOP Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter.