

# Information Security Monthly Activity Report\*

INFOCON LEVEL



February 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)\*\*** ..... x  
**63,899,419**



**Malware (Blocked/Contained)** ..... x x x x x  
**788,159,305**



**Suspicious/Malicious Emails (Blocked)** ..... x x  
**85,677,585**



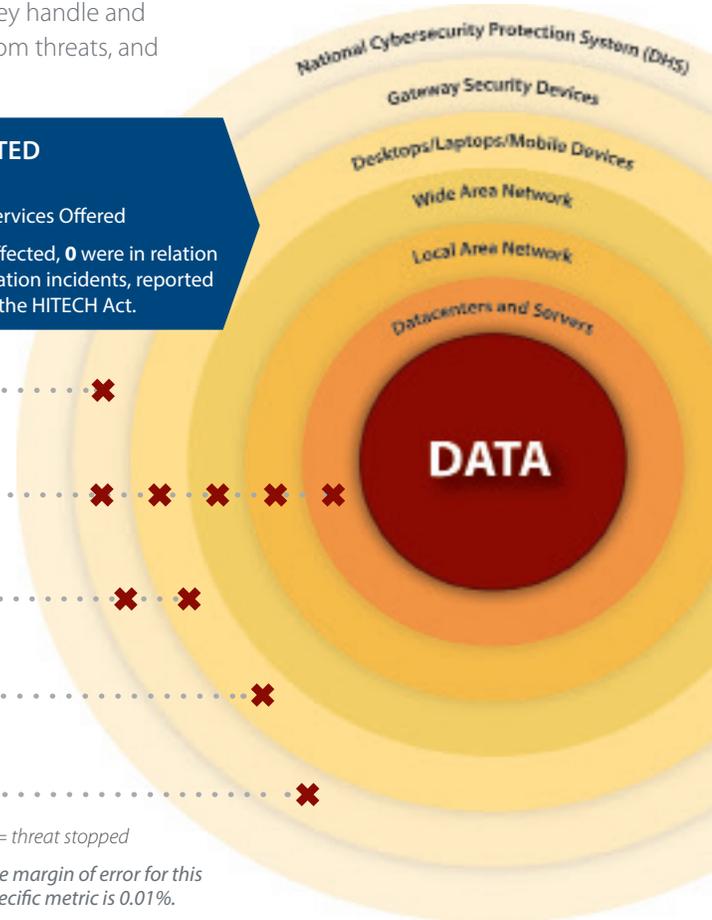
**Infected Medical Devices (Contained)** ..... x  
**1**



**Outgoing Unencrypted Emails** ..... x  
**84** Associated Privacy/Security Events  
**25,514** Total Emails Blocked

x = threat stopped

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



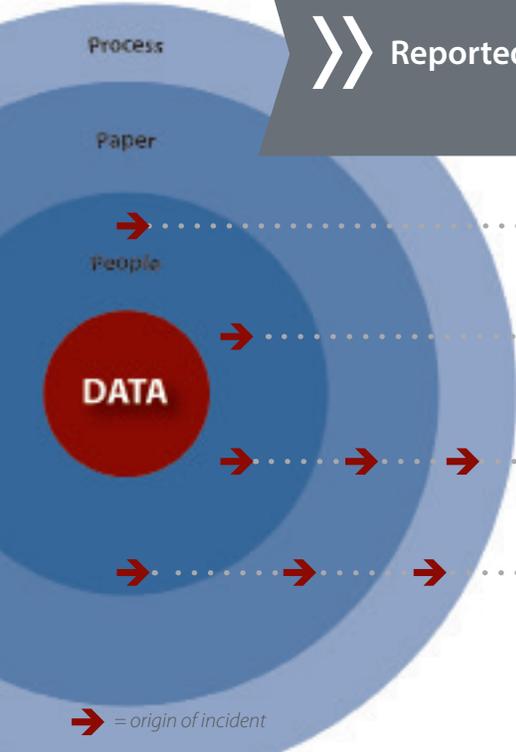
## Reported Events



**817 VETERANS AFFECTED**

- 572 Notifications
- 245 Credit Protection Services Offered

Of the total # of Veterans affected, **707** were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



**Lost and Stolen Device Incidents**  
**43**



**Lost PIV Cards**  
**154**



**Mishandled Incidents**  
**106**



**Mis-mailed Incidents**  
**131** Paper Mis-mailings

**8** Pharmacy-item Mis-mailings  
 out of **6,464,641** 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**  
**February 1 - 29, 2016**

**Security Privacy Ticket Number:** PSETS0000130768

**DBCT Category:** Mismatched

**Organization:** VISN 09  
Lexington, KY

**Date Opened:** 2/1/2016

**Date Closed:** 2/11/2016

**Date of Initial DBCT Review:** N/A

**No. of Credit Monitoring:**

**No. of Loss Notifications:** 1

### **Incident Summary**

Veteran A received Veteran B's medication in the mail which contained full name, home address, and medication type. The medication was returned to the Pharmacy and destroyed.

### **Incident Update**

02/03/16:

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**

The staff has been educated on proper handling of Protected Health Information (PHI), and has taken remedial information security and privacy awareness 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 131 Mis-Mailed incidents this reporting period. Because of repetition, the other 130 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:** PSETS0000130894

**DBCT Category:** Mishandling

**Organization:** VISN 21  
Martinez, CA

**Date Opened:** 2/2/2016

**Date Closed:** 2/23/2016

**Date of Initial DBCT Review:** N/A

**No. of Credit Monitoring:**

**No. of Loss Notifications:** 1

### **Incident Summary**

A VA employee reported that Veteran A returned records pertaining to Veteran B that he received with his requested records.

### **Incident Update**

02/02/16:

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**

Education provided to the employee on importance of reviewing documents before mailing.

### **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 106 Mis-Handling incidents this reporting period. Because of repetition, the other 105 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:** PSETS0000130927  
**DBCT Category:** Unencrypted iPad Missing  
**Organization:** VISN 12  
North Chicago, IL

**Date Opened:** 2/3/2016  
**Date Closed:** 2/22/2016  
**Date of Initial DBCT Review:** N/A

**No. of Credit Monitoring:**  
**No. of Loss Notifications:**

#### **Incident Summary**

VA Doctor A reported to Doctor B that she lost her iPad at a local airport. When she reported the loss to IT Specialist A, he had the Tablet Help Desk send a kill signal to the device. The incident was reported to the Information Security Officer (ISO) on the next day.

#### **Incident Update**

02/22/16:  
The physician did not store any Personally Identifiable Information or Protected Health Information (PII/PHI) on the device. After review and analysis, in accordance with VA Handbook 6500.2, Section 5, § B (Breach Criteria), the Data Breach Response Service has determined that this incident involves a missing data capable device, however the device did not contain any SPI. Therefore no breach has occurred due to the criteria contained in the aforementioned section of VA policy.

#### **Resolution**

It has been confirmed that no PII/PHI was on the device. A kill signal has been sent to the device.

#### **DBCT Decision Date:**

#### **DBCT**

No Data Breach Core Team decision was required. This was left on the report as it is missing unencrypted equipment.

**Security Privacy Ticket Number:** PSETS0000130953  
**DBCT Category:** IT Equipment Inventory  
**Organization:** VISN 02  
Canandaigua, NY

**Date Opened:** 2/3/2016

**Date Closed:** 2/3/2016

**Date of Initial DBCT Review:** 2/9/2016

**No. of Credit Monitoring:**

**No. of Loss Notifications:**

### **Incident Summary**

The facility is currently missing two desktop computers that were recently discovered during an IT inventory.

### **Incident Update**

02/03/16:

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. It was determined that both 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**

It was determined that both desktops were encrypted.

### **DBCT Decision Date:**

### **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 8 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 7 are not included in this report.

**Security Privacy Ticket Number:** PSETS0000131188

**DBCT Category:** Mishandling

**Organization:** VISN 23  
St. Cloud, MN

**Date Opened:** 2/9/2016

**Date Closed:**

**Date of Initial DBCT Review:** 2/23/2016

**No. of Credit Monitoring:**

**No. of Loss Notifications:** 373

### **Incident Summary**

A staff member conducted group meetings to complete a paper packet with four assessments per Veteran in the Mental Health (MH) Outcome Management Program with the Veterans. The assessment results were to be recorded into the Veterans' charts and tracked. The assessment packets cannot be located and were not recorded in the Veterans' charts. The packets contained the Veterans' last name and last four digits of the SSN and multiple choice questions relating to depression, anxiety, brief addiction monitoring, University of Rhode Island Change Assessment (URICA), Behavior And Symptom Identification Scale (Basis 32), and the Posttraumatic Checklist.

### **Incident Update**

02/22/16:

After investigation by the PO, this has been changed from a complaint to an incident. There are a total of 373 Veterans affected. The documents contained last name, last four numbers of the SSN and answers to multiple choice questions regarding mental health issues. The employee does not know if they have been shredded or are just missing.

**DBCT Decision Date:** 02/23/2016

### **DBCT**

02/23/16:

After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Core Team has determined that all 373 Veterans will be sent a HIPAA notification letters due to Protected Health Information (PHI) being disclosed.

**Security Privacy Ticket Number:** PSETS0000131853

**DBCT Category:** CMOP Mismatched

**Organization:** VHA CMOP  
Murfreesboro, TN

**Date Opened:** 2/23/2016

**Date Closed:** 2/26/2016

**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**

02/24/16:

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 2/23/2016, 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 8 Mis-Mailed CMOP incidents out of 6,464,641 total packages (9,557,024 total prescriptions) mailed out for this reporting period. Because of repetition, the other 7 are not included in this report. In all incidents, Veterans will receive a notification letter.