

# Information Security Monthly Activity Report\*

December 2014

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)  
**13,353,776**



Malware (Blocked/Contained)  
**514,502,870**



Suspicious/Malicious Emails (Blocked)  
**99,061,640**



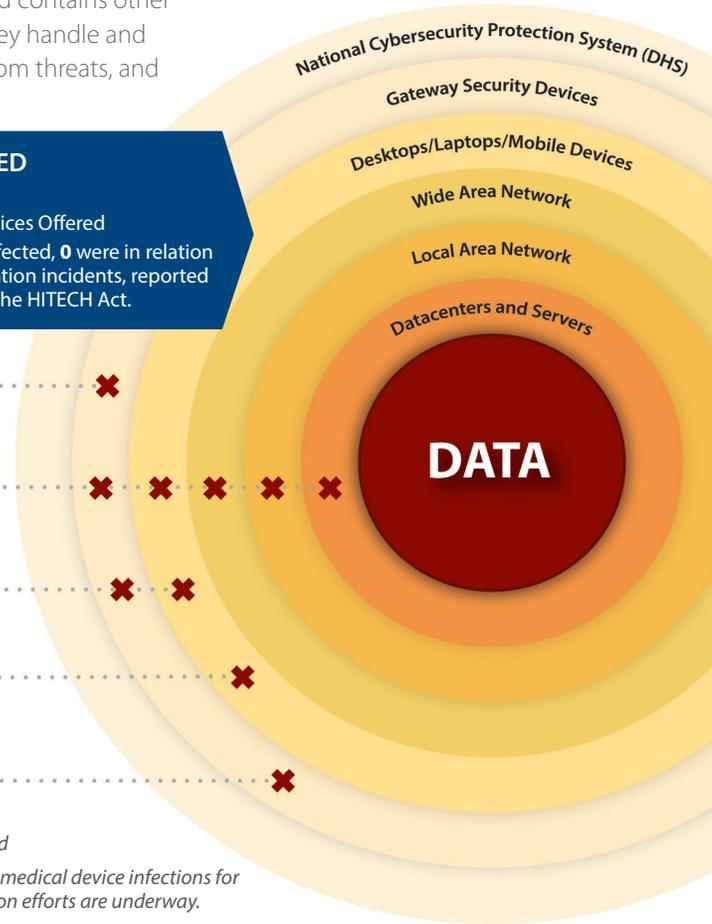
Infected Medical Devices (Contained)\*\*  
**13**



Outgoing Unencrypted Emails (Blocked)  
**91**

✘ = threat stopped

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



## Reported Events



**643 VETERANS AFFECTED**

332 Notifications

311 Credit Protection Services Offered

Of the total # of Veterans affected, **371** were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.

Process

Paper

People

**DATA**



Lost and Stolen Device Incidents  
**51**



Lost PIV Cards  
**120**



Mishandled Incidents  
**116**



Mis-mailed Incidents  
**142**

➔ = 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  
Incident Resolution Service

**Monthly Report to Congress of Data Incidents**  
**December 1 -31, 2014**

**Security Privacy Ticket Number:** PSETS0000112239  
**Incident Type:** Mishandled/ Misused Physical or Verbal Information  
**Organization:** VBA  
Detroit, MI  
**Date Opened:** 12/1/2014  
**Date Closed:** 12/11/2014  
**Date of Initial DBCT Review:** N/A  
**VA-NSOC Incident Number:** VANSOC0613966  
**Date US-CERT Notified:** 12/1/2014  
**US-CERT Case Number:** INC000000421747  
**US-CERT Category:** Category 6 - Investigation  
**No. of Credit Monitoring:** 1  
**No. of Loss Notifications:**  
**DBCT Category:** Mismatched

### **Incident Summary**

Veteran A received the Claim Acknowledgement letter intended for Veteran B, as it was placed in the envelope with Veteran A's information. Veteran A returned the letter for Veteran B to the Battle Creek VA Medical Center. This letter was sent by the VBA Detroit Regional Office.

### **Incident Update**

12/01/14:

The Incident Resolution Service Team has determined that Veteran B will be sent a letter offering credit protection services, as the letter included Veteran B's date of birth.

**Resolution**

Education has been provided to the employee responsible for the incident.

**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 134 Mis-Mailed incidents this reporting period. Because of repetition, the other 133 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:** PSETS0000112260  
**Incident Type:** Missing/Stolen Equipment  
**Organization:** VISN 18  
Albuquerque, NM  
**Date Opened:** 12/1/2014  
**Date Closed:** 12/17/2014  
**Date of Initial DBCT Review:** 12/9/2014  
**VA-NSOC Incident Number:** VANSOC0613986  
**Date US-CERT Notified:** 12/1/2014  
**US-CERT Case Number:** INC000000421867  
**US-CERT Category:** Category 1 - Unauthorized Access  
**No. of Credit Monitoring:**  
**No. of Loss Notifications:**  
**DBCT Category:** IT Equipment Inventory

### **Incident Summary**

Information Resources Management (IRM) staff submitted Reports of Survey (ROS) for the following missing items:

EIL 78C Computers (25 missing)  
EIL 78L Laptops (32 missing)  
EIL 78P Printers (12 missing)

### **Incident Update**

12/03/14:

The facility Chief Information Officer reports that there are no PCs or laptops on the network that are unencrypted.

**Resolution**

The reports of survey were completed on the missing equipment.

**DBCT Decision Date:** 12/09/2014

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

**Security Privacy Ticket Number:** PSETS0000112371  
**Incident Type:** Mishandled/ Misused Physical or Verbal Information  
**Organization:** VISN 08  
Tampa, FL  
**Date Opened:** 12/3/2014  
**Date Closed:** 1/7/2015  
**Date of Initial DBCT Review:** N/A  
**VA-NSOC Incident Number:** VANSOC0614092  
**Date US-CERT Notified:** 12/3/2014  
**US-CERT Case Number:** INC000000422368  
**US-CERT Category:** Category 6 - Investigation  
**No. of Credit Monitoring:** 1  
**No. of Loss Notifications:**  
**DBCT Category:** Mishandling

### **Incident Summary**

Veteran A was given Veteran B's lab paperwork at an outpatient clinic. The information disclosed included Veteran B's full name, full SSN, address, and lab results.

### **Incident Update**

12/03/14:

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

**Resolution**

After an initial investigation it was determined that a physician had printed out the Veteran's lab paperwork and handed the wrong paperwork to the Veteran. The physician was counseled and required to retake his Privacy and HIPAA and VA Privacy and Information Security and Rules of Behavior Training, which was completed on 1/5/2015. The Privacy Office has received the completed certifications for this 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 116 Mis-Handling incidents this reporting period. Because of repetition, the other 115 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:** PSETS0000112501  
**Incident Type:** Mishandled/ Misused Physical or Verbal Information  
**Organization:** VHA CMOP  
Murfreesboro, TN  
**Date Opened:** 12/5/2014  
**Date Closed:** 12/8/2014  
**Date of Initial DBCT Review:** N/A  
**VA-NSOC Incident Number:** VANSOC0614210  
**Date US-CERT Notified:** 12/5/2014  
**US-CERT Case Number:** INC000000423253  
**US-CERT Category:** Category 6 - Investigation  
**No. of Credit Monitoring:**  
**No. of Loss Notifications:** 1  
**DBCT Category:** CMOP Mismatched

### **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. The 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**

12/05/14:

The Incident Resolution Service Team has determined that Patient B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

**Resolution**

On 12/5/14, 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 7,480,927 total packages (10,572,889 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.

**Security Privacy Ticket Number:** PSETS0000113104  
**Incident Type:** Unauthorized Electronic Access  
**Organization:** VISN 03  
New York, NY  
**Date Opened:** 12/22/2014  
**Date Closed:**  
**Date of Initial DBCT Review:** 12/30/2014  
**VA-NSOC Incident Number:** VANSOC0614770  
**Date US-CERT Notified:** 12/22/2014  
**US-CERT Case Number:** INC000000427386  
**US-CERT Category:** Category 4- Improper Usage  
**No. of Credit Monitoring:** 104  
**No. of Loss Notifications:** 1  
**DBCT Category:** Mishandling

### **Incident Summary**

A VA employee notified the facility Privacy Officer (PO) that she sent an email with patient names and SSNs to the wrong recipient. She was sending the information to herself and by accident she sent it to an individual with the same name, but at a Gmail account. She immediately realized the error and she reached out to the individual to ask that she delete the message and she said she immediately deleted it upon receipt. The VA employee notified the PO of the error.

## **Incident Update**

12/24/14:

The PO received the patient list. The report contained 111 unique names. The report was set up to run from Vista. VA sent an email to the Gmail account, but cannot verify if it had been received, opened, read, or deleted. The Gmail account holder called the VA once after responding to our request to delete the message, but she would not leave a contact number. She was a bit hesitant and although the VA emailed her to ask her to delete the report since it was sent to her in error she said she thought she was being hacked and said she may go to her local police. She lead us to believe that she never opened that email because she said she thought it was a scam being sent by an individual with the same name.

12/29/14:

The Incident Resolution Service Team has determined that 111 Veterans will be sent letters offering credit protection services.

01/13/15:

The count of affected individuals has been adjusted due to duplicates and one Veteran was deceased. As of this point, 104 Veterans will be offered credit protection services and 1 Veteran's next of kin will be sent a notification letter.

**DBCT Decision Date:** 12/30/2014

### **DBCT**

DBCT concurs with credit protection services being offered.

**Security Privacy Ticket Number:** PSETS0000113162  
**Incident Type:** Mishandled/ Misused Physical or Verbal Information  
**Organization:** VISN 17  
Dallas, TX  
**Date Opened:** 12/23/2014  
**Date Closed:**  
**Date of Initial DBCT Review:** 12/30/2014  
**VA-NSOC Incident Number:** VANSOC0614823  
**Date US-CERT Notified:** 12/23/2014  
**US-CERT Case Number:** INC000000427977  
**US-CERT Category:** Category 6 - Investigation  
**No. of Credit Monitoring:** 60  
**No. of Loss Notifications:**  
**DBCT Category:** Mishandling

**Incident Summary**

Research consent forms ready for scanning have been determined to be missing. There were a total of 60 subjects involved.

## **Incident Update**

12/23/14:

The PO indicates that they are still searching for the forms.

01/15/15:

At this point the forms cannot be found. The Incident Resolution Service Team has determined that sixty subjects will receive letters offering credit protection services due to full SSN being potentially exposed.

**DBCT Decision Date:** 01/13/2015

## **DBCT**

1/13/15:

The Data Breach Core Team determined that this will require 60 letters offering Credit Protection Services if the consent forms cannot be located.