Information Security
Monthly Activity Report*

INFOCON LEVEL
CRITICAL
SEVERE
ELEVATED
GUARDED
NORMAL

October 2015

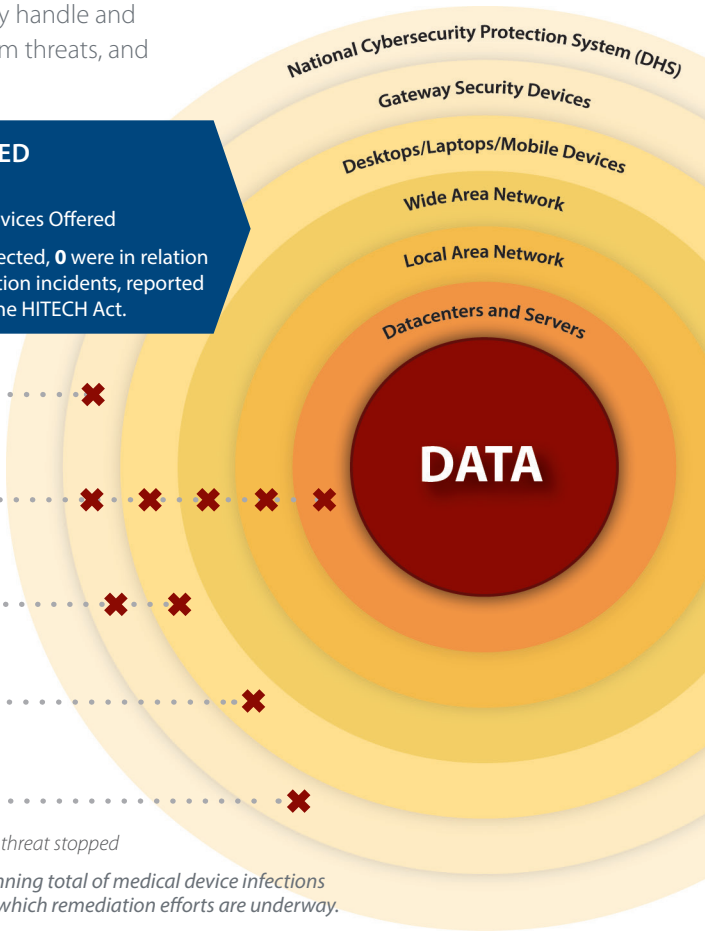
VA uses a defense-in-depth approach to information security to protect the data we hold on Veterans. While the defense-in-depth approach protects from inbound threats and contains other data exposing incidents, VA relies on employees to protect Veteran information they handle and transmit. This graphic 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)
171,819,058

Malware (Blocked/Contained)
585,102,741

Suspicious/Malicious Emails (Blocked)
92,788,709

Infected Medical Devices (Contained)**
0

Outgoing Unencrypted Emails
59 Associated Privacy/Security Events
15,145 Total Emails Blocked

✖ = *threat stopped*

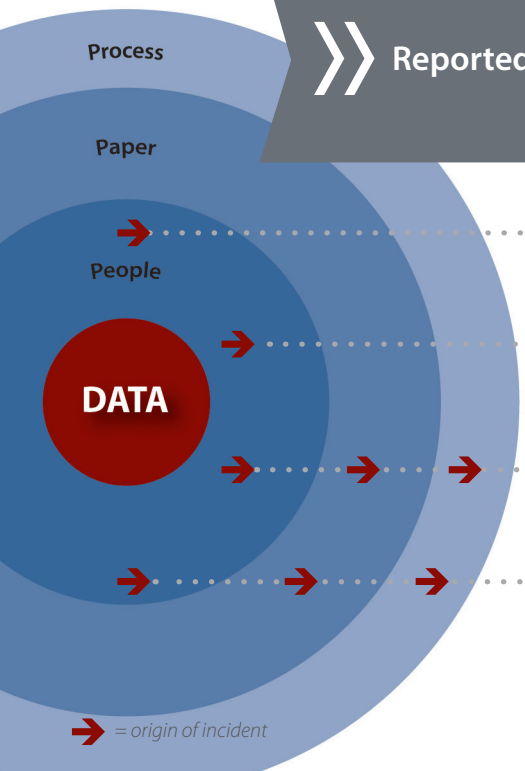
** *Running total of medical device infections for which remediation efforts are underway.*

Reported Events

648 VETERANS AFFECTED

- **363** Notifications
- **285** Credit Protection Services Offered

Of the total # of Veterans affected, **453** were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



Lost and Stolen Device Incidents
49

Lost PIV Cards
158

Mishandled Incidents
81

Mis-mailed Incidents
123 Paper Mis-mailings
8 Pharmacy-item Mis-mailings
out of **7,119,592** 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
Incident Resolution Service

Monthly Report to Congress of Data Incidents

October 1 - 31, 2015

Security Privacy Ticket Number: PSETS0000125397

DBCT Category: Mismailed

Organization: VISN 12
North Chicago, IL

Date Opened: 10/1/2015

Date Closed: 10/13/2015

Date of Initial DBCT Review: 10/6/2015

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

A letter was placed into the incorrect envelope, and sent to wrong patient. The patient returned the letter to the Community Based Outpatient Clinic (CBOC) during the next visit. The Privacy Officer (PO) is unsure how long the patient held on to the letter. The letter is dated 08/04/15.

Incident Update

10/01/15:
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

Supervisor provided training to staff.

DBCT Decision Date: 10/06/2015

DBCT

No DBCT decision is required. This is informational for Mis-Mailed incidents and is the representative ticket. There were a total of 123 Mis-Mailed incidents this reporting period. Because of repetition, the other 122 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: PSETS0000125424

DBCT Category: Mishandling

Organization: VISN 17
San Antonio, TX

Date Opened: 10/1/2015

Date Closed: 10/7/2015

Date of Initial DBCT Review: 10/6/2015

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

Clinic staff gave an appointment list to the wrong Veteran. The Veteran stated he shredded the document. It was not returned to the facility.

Incident Update

10/01/15:
The Incident Resolution Service Team has determined that Veteran B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

Staff re-educated 10-1-15.

DBCT Decision Date: 10/06/2015

DBCT

No DBCT decision is required. This is informational for Mis-Handling incidents and is the representative ticket. There were a total of 81 Mis-Handling incidents this reporting period. Because of repetition, the other 80 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: PSETS0000125453

DBCT Category: IT Equipment Inventory

Organization: VACO OI&T
Washington, DC

Date Opened: 10/2/2015

Date Closed:

Date of Initial DBCT Review: 10/6/2015

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

These items were not located during the FY15 annual inventory for CMR 78T. There were four BlackBerries and two laptops, one iPhone unaccounted for. The remaining twelve items listed on the Report of Survey were not data capable.

Incident Update

10/02/15:
The Incident Resolution Service Team has determined that no data breach occurred, the laptops were encrypted. The BlackBerry and iPhone devices were disabled.

Resolution

DBCT Decision Date: 10/06/2015

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 two IT Equipment Inventory Incidents this reporting period.

Security Privacy Ticket Number: PSETS0000125579

DBCT Category: CMOP Mismailed

Organization: VHA CMOP
Murfreesboro, TN

Date Opened: 10/6/2015

Date Closed: 10/26/2015

Date of Initial DBCT Review: 10/13/2015

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

10/06/15:
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 10/6/15, the CMOP employee was counseled and retrained in proper packing procedures.

DBCT Decision Date: 10/13/2015

DBCT

No DBCT decision is required. This is informational for Mis-Mailed CMOP incidents and is the representative ticket. There was only 8 Mis-Mailed CMOP incident out of 7,119,592 total packages (10,196,596 total prescriptions) mailed out for this reporting period. In this incident, the affected individuals will receive a HIPAA notification letter.

Security Privacy Ticket Number: PSETS0000126004

DBCT Category: Missing/Stolen Equipment (Other)

Organization: VISN 16
Houston, TX

Date Opened: 10/15/2015

Date Closed:

Date of Initial DBCT Review: 10/27/2015

No. of Credit Monitoring:

No. of Loss Notifications: 200

Incident Summary

Nurse reported a digital camera from wound care clinic missing from work area. The camera is a Cannon Powershot ELPH 115-IS. The camera contained a SD card. The data on the camera and SD card was unencrypted. The technician stated the camera contained pictures of patient wounds, last name, and last four of SSN. The digital camera is maintained in a locked cabinet and locked office. However, the technician stated the camera may have been taken from one of the clinics preparatory rooms. Member has reported missing camera to ISO and the ISO will notify the PO due to PII/PHI. The clinic personnel are continuing to look for the camera and inquire with fellow coworkers to ensure camera is missing and not being stored in another location.

Incident Update

10/20/15:
After a search of the clinical area, the camera has not been found. The loss has been reported to the VA Police and the Information Security Office (ISO). The ISO has requested and is awaiting the VA Police Case number to add to the incident ticket. The camera had stored on it photos of wounds along with the last name and last four digits of the patients SSN for 200 patients.

Based on the VA Breach Criteria, all 200 Patients will be sent a HIPAA notification.

The Facility ISO has instructed the Nurse in charge of the camera that pictures are to be removed from the camera and SD card once they have been uploaded into CPRS (patient medical record). Other corrective actions such as a Standard Operating Procedure are being considered by the Facility ISO as well.

DBCT Decision Date: 10/27/2015

DBCT

The Data Breach Core Team concurred with the decision of the Incident Resolution Service Team.

Security Privacy Ticket Number: PSETS0000126258

DBCT Category: Mishandling

Organization: VISN 12
Chicago, IL

Date Opened: 10/22/2015

Date Closed:

Date of Initial DBCT Review: 10/27/2015

No. of Credit Monitoring: 54

No. of Loss Notifications:

Incident Summary

Employee A turned in a Travel log of patients traveling on Shuttle Bus to the Community Based Outpatient Clinic (CBOC). The information on the log was the patient name, full Social Security Number, phone number and the Clinic they attended.

Incident Update

10/22/15:
The driver left the log on the bus and it is not known how long it was there. It was found by a Veteran and given to another bus driver.
The Incident Resolution Service Team has determined that 54 Veterans will be sent a letter offering credit protection services.

DBCT Decision Date: 10/27/2015

DBCT

The Data Breach Core Team concurred with the decision of the Incident Resolution Service Team.

Security Privacy Ticket Number: PSETS0000126401

DBCT Category: Mishandling

Organization: VISN 12
Chicago, IL

Date Opened: 10/26/2015

Date Closed:

Date of Initial DBCT Review: 11/3/2015

No. of Credit Monitoring: 17

No. of Loss Notifications: 38

Incident Summary

A binder containing Veteran PII from a research project dating back to 1991 was found by a visitor in an open unsecured closet located in a construction zone outside of the campus GI clinic. The information contained information from three separate hospitals that participated in the project, including VA.

Incident Update

10/27/15:
Upon Further investigation, the total number of VA patients affected is 55. Seventeen (17) total offers of Credit Protection have been authorized, 7 of which are confirmed, an additional 10 are possible however the status is unknown at this time. Given the date of the research project and the age of the participants at the time of the project, it is believed that they may have since passed away. If the patients are deceased the Next of Kin will be notified. There are 38 affected patients who are deceased and their Next of Kin will be notified.

DBCT Decision Date: 11/03/2015

DBCT

The Data Breach Core Team has concurred that the total number of VA patients affected is 55. Seventeen (17) total offers of Credit Protection have been authorized, 7 of which are confirmed, an additional 10 are possible however the status of those Veterans is unknown at the time of this report. There are 38 affected patients who are deceased and their Next of Kin will be notified.

Security Privacy Ticket Number: PSETS0000126455

DBCT Category:

Organization: VISN 19
Denver, CO

Date Opened: 10/27/2015

Date Closed:

Date of Initial DBCT Review: 11/3/2015

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

VA employee admitted to ISO that he removed some VA sensitive information documents from Denver VAMC in paper form with him when he started working virtually from Pennsylvania last week. Investigation will commence. ISO to report more information after it becomes available.

Incident Update

11/02/15:
Information Security Officer is investigating. The Incident Resolution Service Team requested the ISO to find out:
The number of individuals
Did the employee attempt to seek authorization to remove the paper documents?
How was the employee securing the documents?
Who, besides the employee, would have had access to the documents and did anyone else access the documents?
What is the current disposition of the documents?

DBCT Decision Date:

DBCT

11/03/15:
The Data Breach Core Team is awaiting the investigation results from the Information Security Officer.

Security Privacy Ticket Number:	PSETS0000126625
DBCT Category:	Mishandling
Organization:	VISN 15 Wichita, KS
Date Opened:	10/30/2015
Date Closed:	
Date of Initial DBCT Review:	11/3/2015
No. of Credit Monitoring:	67
No. of Loss Notifications:	

Incident Summary

The Alternate Privacy Officer received a call that a logbook containing multiple SPI was found on a side street exit near a VA Wichita offsite facility. The logbook was found by an Employee/Veteran on October 29, 2015 at around 1:00 p.m. It appears the logbook has been run over multiple times. The Privacy Officer is still determining how long the logbook has been lying in street.

Incident Update

10/30/15:
This was an unapproved logbook. Approximately 60 Veterans' information including their names, dates of birth, full SSNs, lab information, addresses, and other information were in the logbook. It was lost at 9:45 AM on 10/29/15 and was found on the side street at 1:00 PM on the same day. The logbook belonged to a home based primary care worker who was entering all this information on individuals being treated.

11/03/15:
On 10/30/15, additional pages were found near the side street in the tree line, and in a canal that runs beside the street. This brings the total Veterans' information found to 67, though some might not be identifiable. The Privacy Officer (PO) is in the process of typing up all the names of everything found and will check with the employee to see if any items were in the logbook that have not been located. The Incident Resolution Service Team has determined that all 67 Veterans will be offered credit protection services. If additional Veterans' information was involved based on information from the employee who had the logbook, those Veterans will also be offered credit protection services.

DBCT Decision Date: 11/03/2015

DBCT

11/03/15:
The DBCT concurred that this is a breach, and credit monitoring should be offered.