Information Security
Monthly Activity Report*

March 2015

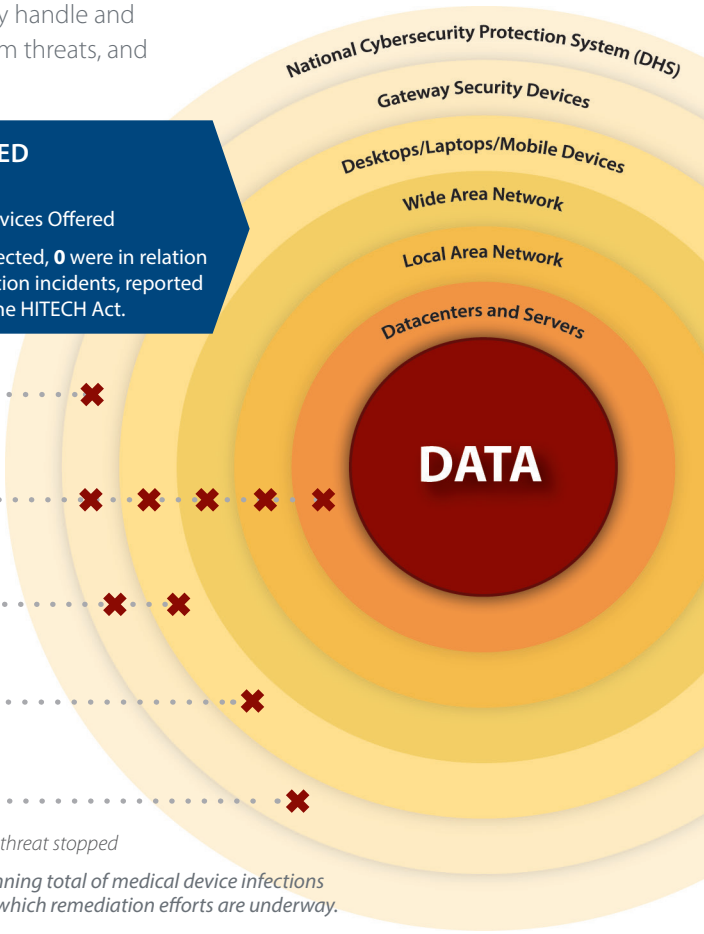
VA uses a defense-in-depth approach to information security to protect the data we hold on Veterans. While the defense-in-depth approach protects from inbound threats and contains other data exposing incidents, VA relies on employees to protect Veteran information they handle and transmit. This graphic 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)
358,163,688

Malware (Blocked/Contained)
1,190,896,611

Suspicious/Malicious Emails (Blocked)
81,343,076

Infected Medical Devices (Contained)**
7

Outgoing Unencrypted Emails
83 Associated Privacy/Security Events
18,589 Total Emails Blocked

✖ = *threat stopped*

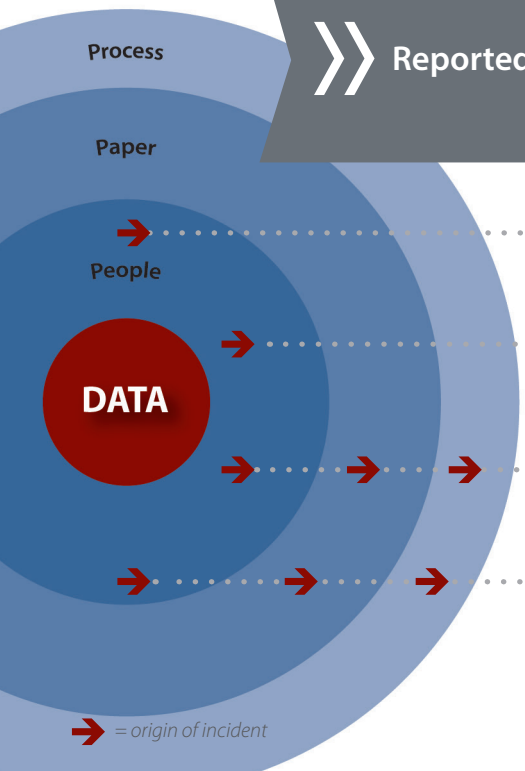
** *Running total of medical device infections for which remediation efforts are underway.*

Reported Events

383 VETERANS AFFECTED

- **159** Notifications
- **224** Credit Protection Services Offered

Of the total # of Veterans affected, **265** were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



Lost and Stolen Device Incidents
50

Lost PIV Cards
154

Mishandled Incidents
105

Mis-mailed Incidents
165 Paper Mis-mailings
7 Pharmacy-item Mis-mailings
out of **7,465,613** 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

March 1-31, 2015

Security Privacy Ticket Number:	PSETS0000116098
DBCT Category:	CMOP Mismailed
Organization:	VHA CMOP Charleston, SC
Date Opened:	3/2/2015
Date Closed:	3/6/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0617675
Date US-CERT Notified:	3/2/2015
US-CERT Case Number:	INC000000446549
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	
No. of Loss Notifications:	1

Incident Summary

Patient A received a Medline Industries medical supply intended for Patient B. Patient B's name and type of medical supply was compromised. Patient A reported the incident to the Grand Junction VA Medical Center (station 575) and the Grand Junction VA Medical Center reported this to the Charleston Consolidated Mail Outpatient Pharmacy (CMOP) on 2/23/15. The CMOP investigation concludes that this was a Medline packing error.

Incident Update

03/02/15:
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

On 3/2/15, the packing error was reported to Medline for investigation and corrective action.

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 7 Mis-Mailed CMOP incidents out of 7,465,613 total packages (10,560,813 total prescriptions) mailed out for this reporting period. Because of repetition, the other 6 are not included in this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number:	PSETS0000116156
DBCT Category:	Mishandling
Organization:	VISN 04 Clarksburg, WV
Date Opened:	3/3/2015
Date Closed:	3/10/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0617732
Date US-CERT Notified:	3/3/2015
US-CERT Case Number:	INC000000446895
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	1
No. of Loss Notifications:	

Incident Summary

Surgery Service printed a copy of an EndoSoft report to the Release of Information (ROI) Office. The ROI clerk was processing a request at the time and attached a copy of Veteran A's Operative Report to Veteran B's request for information. Veteran B picked up the information and left the ROI office in possession of Veteran A's documentation.

Incident Update

03/03/15:
The Incident Resolution Service Team has determined that Veteran A will be sent a letter offering credit protection services.

Resolution

Surgery Service will no longer utilize the printer in ROI to ensure this same error does not happen again.

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 105 Mis-Handling incidents this reporting period. Because of repetition, the other 104 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:	PSETS0000116389
DBCT Category:	Mismailed
Organization:	VBA Denver, CO
Date Opened:	3/9/2015
Date Closed:	3/17/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0617943
Date US-CERT Notified:	3/9/2015
US-CERT Case Number:	INC000000448587
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	1
No. of Loss Notifications:	

Incident Summary

Veteran A contacted the National Call Center (NCC) to say that he received correspondence at his address but the correspondence contained Veteran B's full name and Social Security Number (SSN).

Incident Update

03/09/15:
The Incident Resolution Service Team has determined that Veteran B will be sent a letter offering credit protection services.

Resolution

The employee responsible was counseled on verifying that the employee has the correct Veteran selected prior to making changes to an address. A letter offering credit protection services was mailed on March 17, 2015.

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 165 Mis-Mailed incidents this reporting period. Because of repetition, the other 164 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:	PSETS0000117232
DBCT Category:	IT Equipment Inventory
Organization:	VISN 11 Ann Arbor, MI
Date Opened:	3/26/2015
Date Closed:	
Date of Initial DBCT Review:	3/31/2015
VA-NSOC Incident Number:	VANSOC0618769
Date US-CERT Notified:	3/26/2015
US-CERT Case Number:	INC000000454043
US-CERT Category:	Category 1 - Unauthorized Access
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

As part of the VA Ann Arbor equipment inventory process, excess personal computers were being turned in for disposal by the Research Service. Information Technology staff noted that the four personal computers did not contain any hard drives, and there were no sanitization certificates to state if they were disposed of properly. Two of the computers belong to the University of Michigan, while the other two belong to the VA Ann Arbor Medical Center. None of the systems are managed by the Office of Information and Technology (OI&T). It is unknown what type of information was contained on the hard drives.

Research Service is going to contact the principal investigator that is responsible for the equipment to help determine what the hard drives may contain, and whether the hard drives were encrypted. Research Service has no record of the sanitization certificates.

Incident Update

03/30/15:
The equipment pre-dates the administrative officer for Research, so not much information is available.

04/07/15:
The Research administrative officer is supposed to provide an update this week.

04/14/15:
There were four computers and a bar code reader with a hard drive noted missing. The two VA computers were encrypted and had no patient care data on them. The two computers from the University of Michigan also contained no patient data. The bar code reader was located. The Incident Resolution Service Team has determined that no data breach has occurred.

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 three IT Equipment Inventory incidents this reporting period. Because of repetition, the other two are not included in this report.

Security Privacy Ticket Number:	PSETS0000117266
DBCT Category:	Unencrypted Laptop Missing
Organization:	VISN 07 Montgomery, AL
Date Opened:	3/27/2015
Date Closed:	3/31/2015
Date of Initial DBCT Review:	3/31/2015
VA-NSOC Incident Number:	VANSOC0618799
Date US-CERT Notified:	3/27/2015
US-CERT Case Number:	INC000000454308
US-CERT Category:	Category 1 - Unauthorized Access
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A Prosthetics service laptop has been reported missing.

Incident Update

03/27/15:
The Incident Resolution Service Team has determined that no data breach occurred, as there was no VA sensitive data stored on the laptop. It was not encrypted. The laptop was last inventoried on 03/18/14. It was never connected to the VA network. The ISO advised the service to report the loss to the VA Police.

Resolution

This laptop was 15 years old and was used for programming a prosthetic limb called a C-leg. It could not accept full disk encryption. All current laptops provided by the Office of Information and Technology (OI&T) are encrypted. A VA Police report has been filed.

DBCT Decision Date: 03/31/2015

DBCT

No DBCT decision required. No patient identifiers were stored on the laptop. This incident has been left on the report as it involves missing unencrypted equipment.

Security Privacy Ticket Number:	PSETS0000117273
DBCT Category:	Mishandling
Organization:	VISN 20 Roseburg, OR
Date Opened:	3/27/2015
Date Closed:	
Date of Initial DBCT Review:	3/31/2015
VA-NSOC Incident Number:	VANSOC0618808
Date US-CERT Notified:	3/27/2015
US-CERT Case Number:	INC000000454352
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	70
No. of Loss Notifications:	

Incident Summary

A cooler containing lab specimens being transported by a courier from a VA Community Based Outpatient Clinic (CBOC) did not arrive at the VA Medical Center lab.

Incident Update

03/27/15:
The Privacy Officer (PO) reports that the cooler has been found and all contents are accounted for.

03/30/15:
The VA Police have completed their investigation. Upon review of the final report it was noted that the cooler was found off site in a dumpster. The cooler was in the dumpster for an undetermined amount of time between 3 and 14 hours. The cooler was not secured or monitored during this time period.

04/07/15:
More information has been provided by VA Police and the facility PO. The courier who was supposed to pick up the specimens from the CBOC and deliver to the VA Medical Center lab asked a friend to do it for him. The friend had some personal issues and instead of delivering the documents, threw them in a dumpster near her apartment. The courier has been fired and the friend was taken into police custody.

Due to these circumstances, the Incident Resolution Service, Director has determined that this was a breach and that credit protection services will be offered to the 70 affected Veterans. The Office of General Counsel (OGC) has agreed with that determination. The facility will be asked to recoup expenses from the contractor.

DBCT Decision Date: 04/07/2015

DBCT

03/31/15:
The DBCT has asked if there is language in the contract regarding whose responsibility it is in the case of a data breach.

04/07/15:
There is language in the contract that states the contractor is liable in the event of a breach of confidentiality. After the DBCT meeting on 04/07/15, additional information was received from the facility regarding the circumstances of this incident. Based on this, the Incident Resolution Service, Director determined this was a breach, and it was agreed to by the OGC.

Security Privacy Ticket Number:	PSETS0000117372
DBCT Category:	Unencrypted Laptop Missing
Organization:	VISN 05 Martinsburg, WV
Date Opened:	3/31/2015
Date Closed:	4/16/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0618902
Date US-CERT Notified:	3/31/2015
US-CERT Case Number:	INC000000455255
US-CERT Category:	Category 1 - Unauthorized Access
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

Logistics had received a shipment of 30 laptops. Of those, 16 were assigned and issued to the facility Office of Information and Technology (OI&T) staff and 14 were to be assigned to another group. When the other group came to get the remaining laptops there were only 12. The two unaccounted for laptops were new and were never connected to the VA network and have no VA information on them. The Logistics Department is going back to the vendor to verify that 30 were originally sent and there was no human error. If 30 were shipped, they will be completing a Report of Survey and reporting this to the VA Police.

Incident Update

03/31/15:
The two laptops were new and had no VA information on them, nor had the laptops been connected to the VA network. The Incident Resolution Service Team has determined that no data breach has occurred.

Resolution

A report of survey has been completed and VA Police have been notified.

DBCT Decision Date:

DBCT

No DBCT decision is required. This has been left on the report as it involves missing unencrypted equipment.