Information Security
Monthly Activity Report*

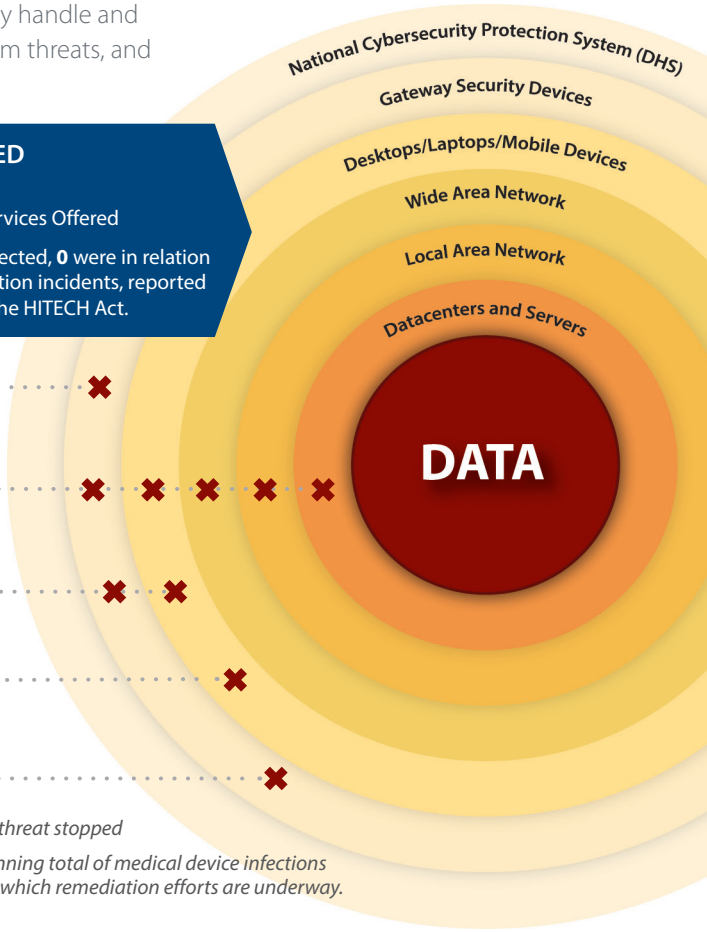
January 2015

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) **14,329,582**
- Malware (Blocked/Contained) **672,920,956**
- Suspicious/Malicious Emails (Blocked) **76,446,478**
- Infected Medical Devices (Contained)** **13**
- Outgoing Unencrypted Emails
  - **90** Associated Privacy/Security Events
  - **20,470** Total Emails Blocked

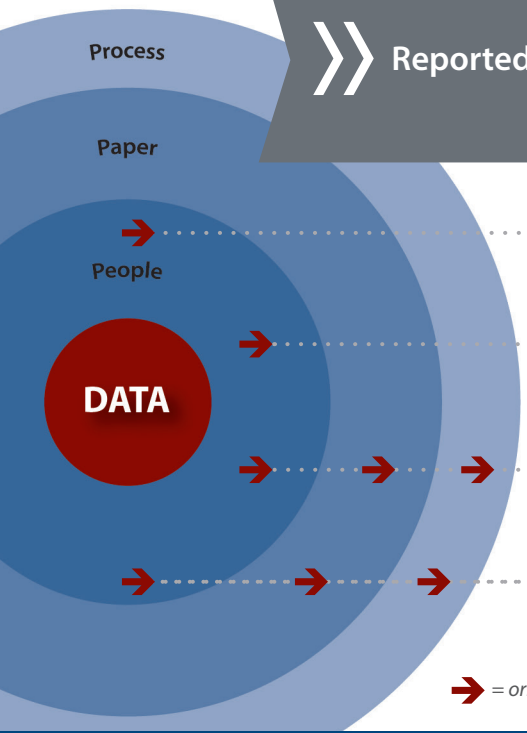
✖ = *threat stopped*

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

Reported Events

310 VETERANS AFFECTED
- **144** Notifications
- **166** Credit Protection Services Offered

Of the total # of Veterans affected, **242** were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



- Lost and Stolen Device Incidents **45**
- Lost PIV Cards **127**
- Mishandled Incidents **92**
- Mis-mailed Incidents **125**

→ = *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

January 1 - 31, 2015

Security Privacy Ticket Number:	PSETS0000113413
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 12 Madison, WI
Date Opened:	1/2/2015
Date Closed:	1/27/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0615078
Date US-CERT Notified:	1/2/2015
US-CERT Case Number:	INC000000429657
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	
No. of Loss Notifications:	1
DBCT Category:	Mishandling

Incident Summary

A pharmacist confused two Veterans' names and had an appointment scheduled for Veteran B, not Veteran A. The appointment list for Veteran B was then handed to Veteran A. The pharmacist contacted Veteran A to retrieve incorrect appointment list.

Incident Update

01/02/15:
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

Staff have been reminded to verify Veteran information before disclosing it outside of VHA, whether to a Veteran or to another entity. Additionally, it was recommended that they complete actions for one Veteran prior to processing another as working with information from multiple Veterans increases the risk of accidental disclosure. The document for Veteran B was returned by Veteran A.

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 92 Mis-Handling incidents this reporting period. Because of repetition, the other 91 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:	PSETS0000113631
Incident Type:	Missing/Stolen Equipment
Organization:	VISN 19 Cheyenne, WY
Date Opened:	1/8/2015
Date Closed:	1/15/2015
Date of Initial DBCT Review:	1/13/2015
VA-NSOC Incident Number:	VANSOC0615284
Date US-CERT Notified:	1/8/2015
US-CERT Case Number:	INC000000431296
US-CERT Category:	Category 1 - Unauthorized Access
No. of Credit Monitoring:	
No. of Loss Notifications:	
DBCT Category:	Unencrypted Laptop Stolen

Incident Summary

A stand-alone laptop was reported missing by a staff member at a Cheyenne VAMC Community Based Out Patient Clinic (CBOC). The laptop has only one application on it that is called "TruthPoint". Once a Veteran has been seen this is the survey that they may take about their appointment. The laptop does not connect to the VA network. A connection is made using a Verizon Wireless MiFi. At no time is there any PHI/PII on this machine. VA Police are conducting an investigation and has notified the OIG of the missing hardware.

Incident Update

01/09/15:
The Incident Resolution Service Team has determined that no data breach has occurred, as no PII or PHI was stored on the device.

01/12/15:
This is not a VA owned laptop. The device, application, and network are contractor owned.

Resolution

Mitigation/Corrective action was issued to the Contracting Officer's Representatives (COR) of the program to order cable locks for these devices.

DBCT Decision Date:

DBCT

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

Security Privacy Ticket Number:	PSETS0000113644
Incident Type:	Missing/Stolen Equipment
Organization:	VISN 04 Wilkes-Barre, PA
Date Opened:	1/9/2015
Date Closed:	1/22/2015
Date of Initial DBCT Review:	1/13/2015
VA-NSOC Incident Number:	VANSOC0615299
Date US-CERT Notified:	1/9/2015
US-CERT Case Number:	INC000000431434
US-CERT Category:	Category 1 - Unauthorized Access
No. of Credit Monitoring:	
No. of Loss Notifications:	
DBCT Category:	IT Equipment Inventory

Incident Summary

PER ISO on 1/9/2015 8:55:46 AM

At approximately 4:00 PM on 1/8/2015 a member of the logistics staff informed the ISO via VA Form 1217, Report of Survey, that two VA Laptops, six desktops, and a biometric VME Biodrive flash drive have not been located during an IT inventory. Initial efforts by the IT staff to locate these devices have not been successful. The ISO was able to locate documentation that one of the laptops had most likely been previously turned in, but with two digits in the EE serial number transposed.

It is believed that all desktop and laptop systems had Symantec Endpoint Encryption installed on them prior to the loss. It is also believed that the VME Biodrive was not actually in use, as when the Biodrive were deemed not FIPS 140-2 compliant, they were taken out of service by the facility IT Service.

Incident Update

01/09/14:
A Report of Survey has been completed.

Resolution

As of 1/22/2015, the CIO and ISO are working on an appropriate mitigation plan.

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 5 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 4 are not included in this report.

Security Privacy Ticket Number:	PSETS0000114170
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 16 Little Rock, AR
Date Opened:	1/22/2015
Date Closed:	2/6/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0615826
Date US-CERT Notified:	1/22/2015
US-CERT Case Number:	INC000000435111
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	
No. of Loss Notifications:	2
DBCT Category:	Mismailed

Incident Summary

Two Veterans with the same last name received each other's medication in the mail. Information exposed was the Veteran's name, address and prescription label. They both returned the inappropriate medications and were given the correct medications.

Incident Update

01/22/15:
The Incident Resolution Service Team has determined that two Veterans will be sent HIPAA notification letters due to Protected Health Information (PHI) being disclosed.

Resolution

Letters were sent out to the Veterans that explained the error regarding their medications. The Veterans had same last name. Employees were required to retake training again. Local management has been made aware of the incident.

PO sent a Request for Information (RFI) asking for additional assistance in helping to have such issues be controlled.

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 118 Mis-Mailed incidents this reporting period. Because of repetition, the other 117 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:	PSETS0000114252
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VHA CMOP Hines, IL
Date Opened:	1/23/2015
Date Closed:	2/4/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0615929
Date US-CERT Notified:	1/23/2015
US-CERT Case Number:	INC000000435651
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	
No. of Loss Notifications:	1
DBCT Category:	CMOP Mismailed

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 Great Lakes 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

01/23/15:
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 1/23/15, 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 7 Mis-Mailed CMOP incidents out of 7,189,315 total packages (10,232,524 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.