Information Security
Monthly Activity Report*

May 2015

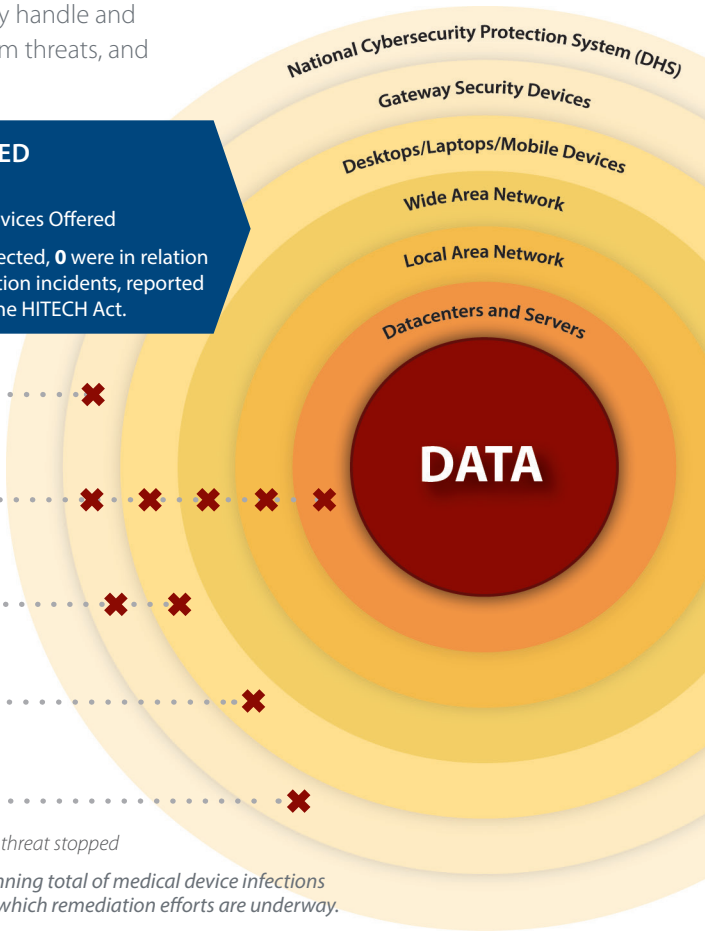
VA uses a defense-in-depth approach to information security to protect the data we hold on Veterans. While the defense-in-depth approach protects from inbound threats and contains other data exposing incidents, VA relies on employees to protect Veteran information they handle and transmit. This graphic 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)
336,455,268

Malware (Blocked/Contained)
574,703,578

Suspicious/Malicious Emails (Blocked)
73,986,996

Infected Medical Devices (Contained)**
2

Outgoing Unencrypted Emails
86 Associated Privacy/Security Events
13,457 Total Emails Blocked

✖ = *threat stopped*

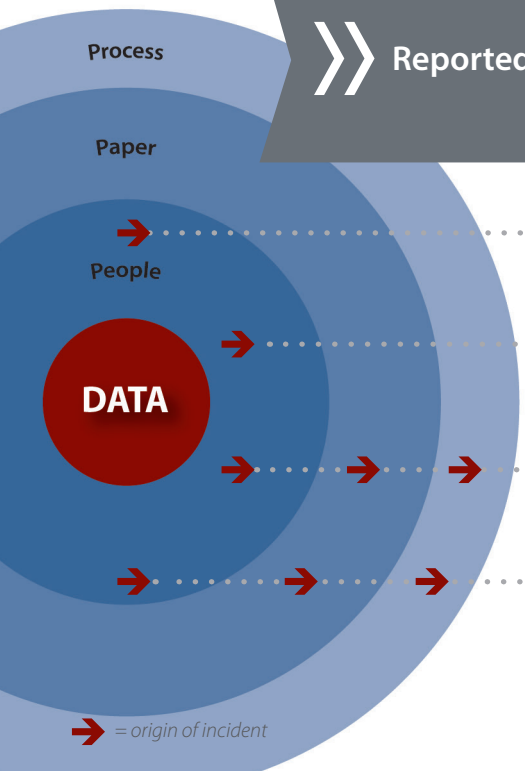
** *Running total of medical device infections for which remediation efforts are underway.*

Reported Events

1,018 VETERANS AFFECTED

- **303** Notifications
- **715** Credit Protection Services Offered

Of the total # of Veterans affected, **361** were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



Lost and Stolen Device Incidents
60

Lost PIV Cards
134

Mishandled Incidents
100

Mis-mailed Incidents
162 Paper Mis-mailings
22 Pharmacy-item Mis-mailings
out of **6,676,699** 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
Incident Resolution Service

Monthly Report to Congress of Data Incidents

May 1-31, 2015

Security Privacy Ticket Number:	PSETS0000119467
DBCT Category:	IT Equipment Inventory
Organization:	VISN 23 Iowa City, IA
Date Opened:	5/13/2015
Date Closed:	5/14/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0620888
Date US-CERT Notified:	5/13/2015
US-CERT Case Number:	INC000000468064
US-CERT Category:	Category 1 - Unauthorized Access
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

During a routine inventory of VA engineering equipment, it was found that one Dell desktop computer capable of storing VA data could not be located. It is unknown if the hard drive was encrypted or tracking software was deployed on the device, however the device was not used to store or transmit sensitive data.

Incident Update

05/14/15:
The Incident Resolution Service Team has determined that no data breach has occurred. The workstation did not contain or transmit any sensitive data.

Resolution

A report of survey has been started for the device and VA Police were contacted as part of the report of survey team.

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 4 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 3 are not included in this report.

Security Privacy Ticket Number:	PSETS0000119530
DBCT Category:	Unencrypted Laptop Missing
Organization:	VISN 19 Fort Harrison, MT
Date Opened:	5/14/2015
Date Closed:	5/29/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0620953
Date US-CERT Notified:	5/14/2015
US-CERT Case Number:	INC000000468473
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

The Information Security Officer (ISO) and Fiscal Department were notified on 05/13/15 of a Samsung Galaxy tablet belonging to the Women's Health Project that was mailed to the wrong Community Based Outpatient Clinic (CBOC) location, and could not be located after 03/30/15.

Incident Update

05/18/15:
The tablet was neither encrypted nor connected to the VA network and did not contain any sensitive VA data. No breach has occurred.

Resolution

Tablets will have now labels on them warning users not to enter or store any sensitive information on them. Also, users will be reinstructed to contact the ISO as soon as one is known to be missing.

DBCT Decision Date:

DBCT

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

Security Privacy Ticket Number:	PSETS0000119811
DBCT Category:	Mishandling
Organization:	VBA Portland, OR
Date Opened:	5/21/2015
Date Closed:	6/1/2015
Date of Initial DBCT Review:	5/26/2015
VA-NSOC Incident Number:	VANSOC0621229
Date US-CERT Notified:	5/21/2015
US-CERT Case Number:	INC000000470328
US-CERT Category:	Category 4- Improper Usage
No. of Credit Monitoring:	508
No. of Loss Notifications:	

Incident Summary

A Vocational Rehabilitation and Employment (VR&E) employee emailed 508 Veteran names and SSNs incorrectly to an outside entity. The information was on a spreadsheet. The individual who received the information was a Veteran who was a client of the VR&E employee.

Incident Update

05/21/15:
The Incident Resolution Service Team has determined that 508 Veterans will be sent a letter offering credit protection services.

Resolution

The VR&E employee was counseled by the supervisor.

DBCT Decision Date: 05/26/2015

DBCT

05/26/2015:
This incident was briefed to the DBCT due to the numbers of individuals involved. The DBCT concurred that 508 Veterans will be offered credit protection services.

Security Privacy Ticket Number:	PSETS0000119835
DBCT Category:	Mishandling
Organization:	VISN 11 Ann Arbor, MI
Date Opened:	5/21/2015
Date Closed:	
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0621251
Date US-CERT Notified:	5/21/2015
US-CERT Case Number:	INC000000470413
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	29
No. of Loss Notifications:	

Incident Summary

An Ambulatory Care Medical Support Assistant (MSA) was given a Patient Treatment File (PTF) Patient List along with patient labs by an RN and instructed to fax the documents to the patient. The PTF list included 29 inpatient full names, full SSNs, location in facility, doctor's name, and home phone number.

Incident Update

05/22/15:
The Incident Resolution Service Team has determined that the 29 Veterans whose information was disclosed will be sent letters offering credit protection services.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for Mishandling incidents and is the representative ticket. There were a total of 100 Mishandling incidents this reporting period. Because of repetition, the other 99 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:	PSETS0000119968
DBCT Category:	CMOP Mismailed
Organization:	VHA CMOP Tucson, AZ
Date Opened:	5/27/2015
Date Closed:	6/2/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0621379
Date US-CERT Notified:	5/27/2015
US-CERT Case Number:	INC000000471544,
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	
No. of Loss Notifications:	15

Incident Summary

Fifteen patient's received a Consolidated Mail Outpatient Pharmacy (CMOP) prescription package intended for fifteen other patient's. Fifteen patient's name and type of medication were disclosed. No SSN data was compromised. The Patients reported the incident to the medical center and a replacement has been requested for Patients whose medications were mismailed. The Tucson CMOP investigation concludes that this was a mail consolidator error. The packing labels were misapplied to the packages. The mail consolidator has been notified of the error and will take corrective action.

Incident Update

05/27/15:
The Incident Resolution Service Team has determined that 15 Veterans will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

On 5/27/15, the mail consolidator was notified of the error and will take corrective action.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for Mismailed CMOP incidents and is the representative ticket. There were a total of 22 Mismailed CMOP incidents out of 6,676,699 total packages (9,954,473 total prescriptions) mailed out for this reporting period. Because of repetition, the other 21 are not included in this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number:	PSETS0000119995
DBCT Category:	Mismailed
Organization:	VBA Milwaukee, WI
Date Opened:	5/27/2015
Date Closed:	5/28/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0621408
Date US-CERT Notified:	5/27/2015
US-CERT Case Number:	INC000000471659
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	1
No. of Loss Notifications:	

Incident Summary

A letter addressed to Veteran A was included in the correspondence package sent to and recieved by Veteran B.

Incident Update

05/27/15:
The Incident Resolution Service Team has determined that Veteran A will be sent a letter offering credit protection services.

Resolution

The employee responsible for the mismailing was re-educated on proper procedures on 05/28/15.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for Mismailed incidents and is the representative ticket. There were a total of 162 Mismailed incidents this reporting period. Because of repetition, the other 161 are not included in this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.