Information Security
Monthly Activity Report*

INFOCON LEVEL
CRITICAL
SEVERE
ELEVATED
GUARDED
NORMAL

July 2015

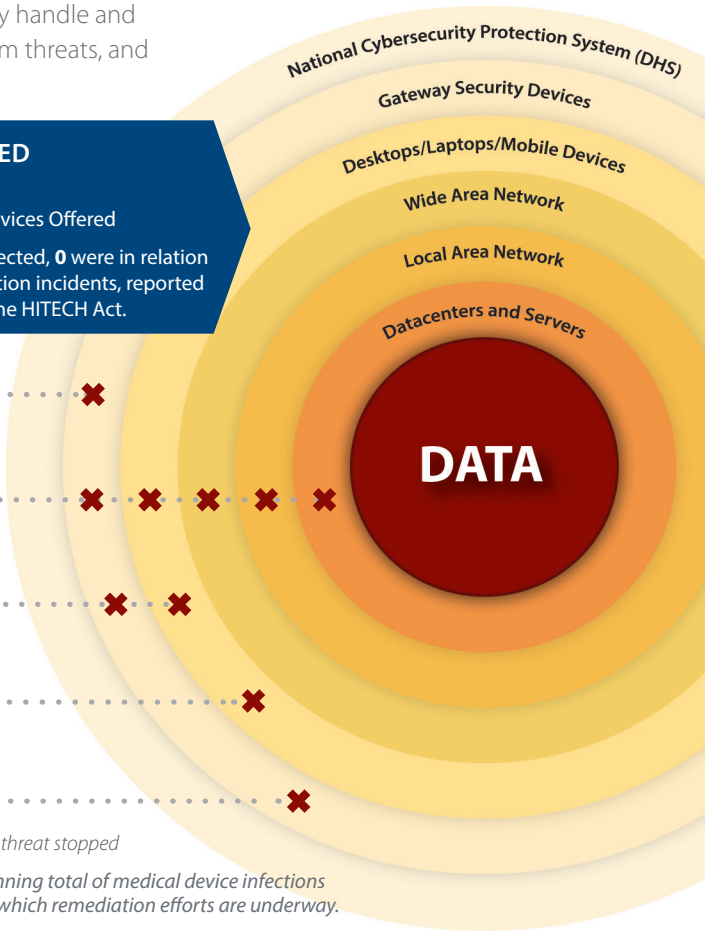
VA uses a defense-in-depth approach to information security to protect the data we hold on Veterans. While the defense-in-depth approach protects from inbound threats and contains other data exposing incidents, VA relies on employees to protect Veteran information they handle and transmit. This graphic 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)
319,989,878

Malware (Blocked/Contained)
791,111,239

Suspicious/Malicious Emails (Blocked)
104,377,769

Infected Medical Devices (Contained)**
1

Outgoing Unencrypted Emails
70 Associated Privacy/Security Events
15,701 Total Emails Blocked

✖ = *threat stopped*

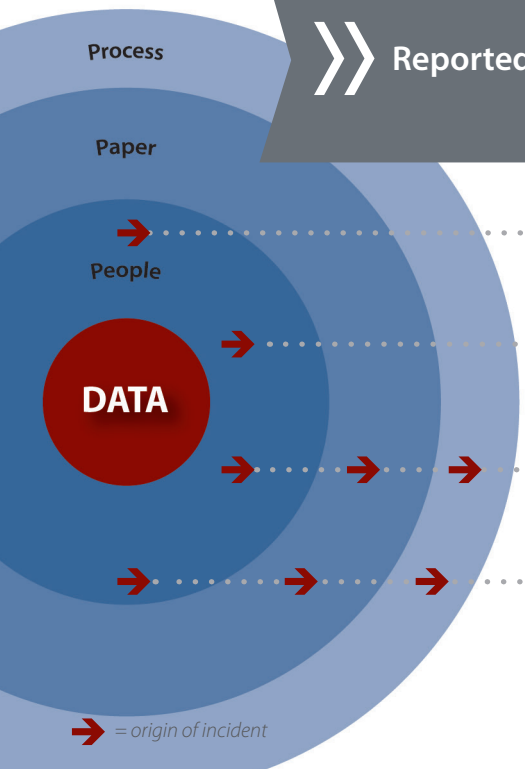
** *Running total of medical device infections for which remediation efforts are underway.*

Reported Events

1,031 VETERANS AFFECTED

- **779** Notifications
- **252** Credit Protection Services Offered

Of the total # of Veterans affected, **872** were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



Lost and Stolen Device Incidents
56

Lost PIV Cards
160

Mishandled Incidents
111

Mis-mailed Incidents
158 Paper Mis-mailings
27 Pharmacy-item Mis-mailings
out of **7,384,239** 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

July 1-31, 2015

Security Privacy Ticket Number:	PSETS0000121597
DBCT Category:	CMOP Mismailed
Organization:	VHA CMOP Charleston, SC
Date Opened:	7/1/2015
Date Closed:	
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0622983
Date US-CERT Notified:	7/1/2015
US-CERT Case Number:	INC000010009755
US-CERT Category:	Category 6 - Investigation
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 Atlanta VA Medical Center (Site 508) and a replacement has been requested for Patient B. The Charleston 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

07/01/15:
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.

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 27 Mismailed CMOP incidents out of 7,384,239 total packages (10,533,694 total prescriptions) mailed out for this reporting period. Because of repetition, the other 26 are not included in this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number:	PSETS0000121628
DBCT Category:	Mismailed
Organization:	VISN 21 Honolulu, HI
Date Opened:	7/1/2015
Date Closed:	7/2/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0623015
Date US-CERT Notified:	7/1/2015
US-CERT Case Number:	INC000010009910
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	1
No. of Loss Notifications:	

Incident Summary

A provider referral for outside medical care was intended to be mailed to Veteran A. It was sent in error to Veteran B. When Veteran B received this he immediately brought it in.

Incident Update

07/01/15:
The Incident Resolution Service Team has determined that Veteran A will be sent a letter offering credit protection services, as his full name, full SSN, and other information was disclosed inappropriately.

Resolution

Privacy training was provided to staff as a result of this incident.

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 158 Mismailed incidents this reporting period. Because of repetition, the other 157 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:	PSETS0000121805
DBCT Category:	Mishandling
Organization:	VISN 17 San Antonio, TX
Date Opened:	7/7/2015
Date Closed:	7/13/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0623193
Date US-CERT Notified:	7/7/2015
US-CERT Case Number:	INC000010011354
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	1
No. of Loss Notifications:	

Incident Summary

Veteran A was given Veteran B's pulmonary after-visit summary note. The clinic will retrieve the document.

Incident Update

07/07/15:
The Incident Resolution Service Team has determined that Veteran B will be sent a letter offering credit protection services.

Resolution

The employee responsible was re-educated 07/07/15.

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 111 Mishandling incidents this reporting period. Because of repetition, the other 110 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:	PSETS0000121994
DBCT Category:	Mishandling
Organization:	VISN 03 Northport, NY
Date Opened:	7/10/2015
Date Closed:	8/7/2015
Date of Initial DBCT Review:	7/14/2015
VA-NSOC Incident Number:	VANSOC0623377
Date US-CERT Notified:	7/10/2015
US-CERT Case Number:	INC000010012236
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	
No. of Loss Notifications:	89

Incident Summary

A dental student tore pages out of a procedure/prep book which contains names, last four digits of the SSN, and the dental procedures of Veterans. When asked why the pages were torn out, the dental student replied that he put the pages in the burn box. Upon further investigation, it was found that the pages were not in the burn box and therefore it is questionable as to what happened to these pages. The student has since left the program.

Incident Update

07/13/15:
The Privacy Officer states that the log books contain last name, last four numbers of the Social Security Number, and dental procedure. Approximately 89 patients were listed on the pages.

07/13/15:
The Incident Resolution Service Team has determined that 89 Veterans will be sent a notification letter.

Resolution

Letters have been sent out to all Veterans in the dental clinic. Employee has since separated from service and VA Police are continuing their investigation into the matter.

DBCT Decision Date: 07/14/2015

DBCT

07/14/15:
The DBCT concurs that this is a data breach.

Security Privacy Ticket Number:	PSETS0000122500
DBCT Category:	Mishandling
Organization:	VISN 16 Houston, TX
Date Opened:	7/23/2015
Date Closed:	
Date of Initial DBCT Review:	7/28/2015
VA-NSOC Incident Number:	VANSOC0623933
Date US-CERT Notified:	7/24/2015
US-CERT Case Number:	INC000010016177
US-CERT Category:	Category 4- Improper Usage
No. of Credit Monitoring:	26
No. of Loss Notifications:	391

Incident Summary

As part of an ongoing investigation of a VA employee, an allegation has been made that this employee used his VA Outlook account to send sensitive information outside the VA. The Privacy Officer (PO) has been asked to investigate and make a determination whether any privacy and or security rules have been violated.

Incident Update

07/24/15:
After reviewing the emails, the PO confirmed that the physician sent emails containing Veteran's individually identifiable information and protected health information outside the VA to his personal Yahoo email account and another email account that has not yet been identified. Twenty Six Veterans' full name and SSN were disclosed. Another 391 Veterans had their names and other information (not including the full SSN or date of birth) disclosed in the emails.

07/26/15:
It is unknown if he forwarded the emails from the Yahoo account to any one or downloaded them to a private computer.

07/28/15:
The Incident Resolution Service Team and the DBCT has determined that twenty-six Veterans will receive a letter offering credit protections services and 391 will receive notification letters.

Resolution

Findings letter sent to labor management specialist for appropriate disciplinary action.

DBCT Decision Date: 07/28/2015

DBCT

DBCT concurred that this is a breach.

Security Privacy Ticket Number:	PSETS0000122801
DBCT Category:	Unencrypted iPad Stolen
Organization:	VISN 19 Cheyenne, WY
Date Opened:	7/30/2015
Date Closed:	
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0624119
Date US-CERT Notified:	7/30/2015
US-CERT Case Number:	INC000010017709
US-CERT Category:	Category 1 - Unauthorized Access
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

On 07/29/15 at approximately 6:00 PM, a VA employee unloaded VA issued hardware from government owned vehicle to the employee’s personal vehicle after her tour of duty was over. The employee stopped at a store on the way home and while in the store someone broke into the employee's vehicle and took the following VA issued equipment: an iPad, cell phone, PIV, and car key. The employee's personal laptop was stolen as well. The employee notified the local police department and VA Police Service and both have taken statements along with police reports. The wireless carrier was notified and shut off cell service to the iPad and cell phone.

Incident Update

07/30/15:
The laptop is a personal laptop of the employee. It was used to log into the VA network when seeing patients in the field. There is no encryption on the physical machine since it is not VA owned equipment. VA data was not downloaded from the network onto the laptop. The VA iPad is not encrypted but was password protected. IT Staff have submitted a ticket to have the iPad remotely erased. The account for remote access has been disabled for this user.

DBCT Decision Date:

DBCT

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