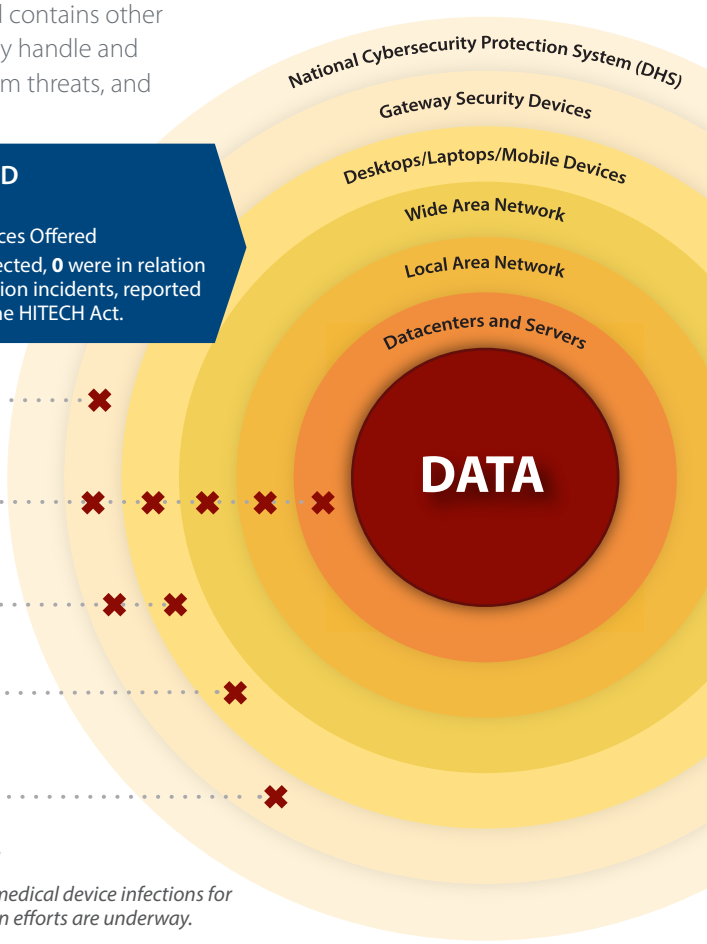
Information Security
Monthly Activity Report*

November 2014

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.



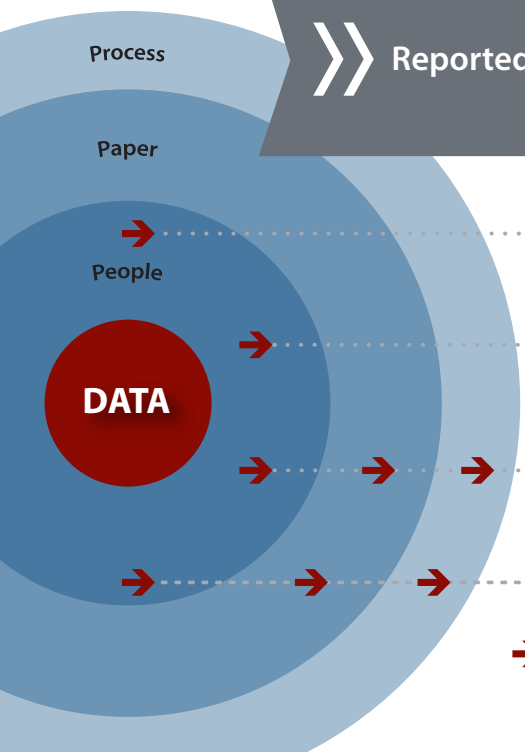
- Intrusion Attempts (Blocked) **15,197,616**
- Malware (Blocked/Contained) **328,682,034**
- Suspicious/Malicious Emails (Blocked) **88,065,600**
- Infected Medical Devices (Contained)** **4**
- Outgoing Unencrypted Emails (Blocked) **57**

✖ = *threat stopped*

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

Reported Events

8,733 VETERANS AFFECTED
179 Notifications
8,554 Credit Protection Services Offered
Of the total # of Veterans affected, **1430** were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



- Lost and Stolen Devices **39**
- Lost PIV Cards **110**
- Mishandled Incidents **81**
- Mis-mailed Incidents **102**

→ = *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

November 1 - 30, 2014

Security Privacy Ticket Number:	PSETS0000111316
Incident Type:	Mishandled/ Misused Electronic Information
Organization:	Corporate Data Center Operations (CDCO) Austin, TX
Date Opened:	11/5/2014
Date Closed:	11/17/2014
Date of Initial DBCT Review:	11/18/2014
VA-NSOC Incident Number:	VANSOC0613061
Date US-CERT Notified:	11/5/2014
US-CERT Case Number:	INC000000415392
US-CERT Category:	Category 4- Improper Usage
No. of Credit Monitoring:	7463
No. of Loss Notifications:	
DBCT Category:	Mishandling

Incident Summary

A public facing website which is run by a VA contractor for VHA Telehealth has been found to have a vulnerability. If someone knew a specific URL, they could have potentially accessed a document which contained personally identifiable information (PII) of several thousand VA patients. The URL was very specific and it would have had to have been typed into the web browser to be accessed, but there is a possibility it could have been. The vulnerability was open for several years.

An anonymous email regarding the vulnerabilities and other issues had been sent to VA leadership. The email contained five Veterans' PII.

Incident Update

11/13/14:
During follow-up conference calls regarding this incident, it was discussed that while the link was accessible on the internet to the public, if one did not know the link was there, it would not be accessed. The vendor stated the anonymous email with data (name, SSN, date of birth) on five home telehealth patients was believed to have been sent by a vendor employee that was terminated during their investigation. That employee did have authorized access to the information. The information was emailed to VA leadership. The OIG has reviewed the incident and declined investigation due to the lack of evidence substantiating any wrong doing or access by the public.

11/17/14:
The website was scanned by the VA Network and Security Operations Center (NSOC) and the NSOC worked together with the vender to fix the vulnerability. According to the vendor, scans and a review of logs have shown that there was no inappropriate access to the web site and no Veteran data was compromised.

However, it has since been alleged that a vendor employee accessed the website or database and copied information regarding five Veterans and emailed the information to the several VA executives. The vendor conducted an investigation and identified one employee who they believe sent this information from an anonymous Gmail account. VA does not know if the employee still has the data in his possession. VA also does not know if the employee would have saved the entire database of several thousand Veterans or just the five Veterans. The employee accused has denied taking any data and has denied ever sending the email.

12/01/2014:
The VA NSOC was asked to review the logs that the vendor stated showed no appropriate access to the web site and that no data was compromised. What follows is a summary of the responses NSOC provided regarding their findings:

1) NSOC cannot verify that the logs are complete. For an official review, NSOC would need to pull the logs, instead of vendor staff.
2) The logs do not show the external IPs, they only show the internal IPs when someone accesses the page from the Internet.
3) Referrers and user agents can be spoofed.
4) Some external IP accesses appear to be from the vendor, as they are accessing the vendor's support page.
5) Other external accesses cannot be verified by the NSOC to be vendor accesses.
6) If the vendor has additional information on how they determined these were vendor accesses, NSOC could review that.
7) Some logs only go back one year.
8) There is no way for NSOC to determine with 100% certainty who could have accessed this page based only on the logs.
9) Besides this issue, VA should look more into the data exposure caused by the vendor employee that allegedly took VA data out of the VA network and emailed it with a Gmail account.

12/02/14:
The Data Breach Core Team reviewed the incident and determined that based on the input from the NSOC, the fact that the link was open for a matter of years, and the amount of unanswered questions regarding the email sent to VA leadership, the risk is high enough to consider this a data breach and offer credit monitoring services for all individuals in the database. The logs do show that the link was accessed; however, there is no way to know who accessed the information. The information which was gained and put in the email creates a further risk in that an individual accessed and exposed the information, however, the VA does not definitively know who accessed the information or if it is still in their possession. Letters offering credit monitoring services will be sent to 7,463 Veterans.

Resolution

The website vulnerability has been remediated.

DBCT Decision Date: 12/02/2014

DBCT

The DBCT determined the incident to be more than a low risk, based on the website vulnerability, the NSOC review, and unanswered questions regarding the email sent to VA leadership. Credit protection services will be offered to 7,463 Veterans.

Security Privacy Ticket Number:	PSETS0000111390
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 07 Montgomery, AL
Date Opened:	11/6/2014
Date Closed:	12/1/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0613132
Date US-CERT Notified:	11/6/2014
US-CERT Case Number:	INC000000415782
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	9
No. of Loss Notifications:	
DBCT Category:	Mishandling

Incident Summary

A phlebotomist went to collect specimens in the facility and lost the lab order list that contained patients' sensitive information while on her rounds.

Incident Update

11/06/14:
The Incident Resolution Service Team has determined that eight Veterans will be sent a letter offering credit protection services.

11/10/14:
The Privacy Officer corrected the count. Nine Veterans were involved and will be sent a letter offering credit protection services.

Resolution

The staff member has been retrained on protecting patient information and the procedure for collecting specimens was reinforced.

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 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:	PSETS0000111626
Incident Type:	Missing/Stolen Equipment
Organization:	VISN 09 Nashville, TN
Date Opened:	11/13/2014
Date Closed:	11/13/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0613340
Date US-CERT Notified:	11/13/2014
US-CERT Case Number:	INC000000417573
US-CERT Category:	Category 1 - Unauthorized Access
No. of Credit Monitoring:	
No. of Loss Notifications:	
DBCT Category:	Unencrypted Laptop Missing

Incident Summary

Computer equipment was ordered by central office for a surgical project located at the Nashville VAMC Surgical Service operating room. The equipment was received in September, 2012. The project was not underway at the time of receipt. The equipment was sent to the Murfreesboro VAMC campus for storage within a couple days of receipt. Nashville VAMC staff were notified in October, 2014 that the project was halted. At that point, Nashville staff asked for the equipment to be returned from Murfreesboro to be used. All equipment received was returned to Nashville except for one laptop. IT staff attempted to locate it on the network unsuccessfully. On further investigation, the laptop was never placed on the VA network. Once the laptop was checked in, it remained in the shipping box for storage.

Incident Update

11/13/14:
The Incident Resolution Service Team has determined that no data breach has occurred. The laptop did not contain any data. It was never powered on and never taken out of the original packaging.

Resolution

A Report of Survey and a VA Police Report have been filed.

DBCT Decision Date:

DBCT

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

Security Privacy Ticket Number:	PSETS0000111659
Incident Type:	Missing/Stolen Equipment
Organization:	VBA Reno, NV
Date Opened:	11/14/2014
Date Closed:	11/17/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0613373
Date US-CERT Notified:	11/14/2014
US-CERT Case Number:	INC000000417831
US-CERT Category:	Category 1 - Unauthorized Access
No. of Credit Monitoring:	
No. of Loss Notifications:	
DBCT Category:	IT Equipment Inventory

Incident Summary

OIT has lost track of a wireless cellular network card. During a recent inventory of IT equipment it was discovered that and device was unaccounted for and the location is unknown.

Incident Update

11/14/14:
The Incident Resolution Service Team has determined that no data breach has occurred, as this equipment is not data storage capable.

Resolution

The employee who reported the loss has reviewed all areas and interviewed individuals to try to locate the device, but was unable to find it. The employee states that the item is lost and has notified all appropriate parties.

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 two IT Equipment Inventory Incidents this reporting period. Because of repetition, the other one is not included in this report.

Security Privacy Ticket Number:	PSETS0000111684
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 07 Columbia, SC
Date Opened:	11/14/2014
Date Closed:	
Date of Initial DBCT Review:	11/18/2014
VA-NSOC Incident Number:	VANSOC0613395
Date US-CERT Notified:	11/14/2014
US-CERT Case Number:	INC000000417930
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	1081
No. of Loss Notifications:	
DBCT Category:	Mishandling

Incident Summary

A Veteran brought a stack of papers to a clerk at the check-in window. The Veteran stated he was looking through the magazines on one of the tables in the White Team waiting area and came across the papers. He turned them in because the papers included full names, social security numbers, and other information. The papers appeared to be a 20 page report printed on both sides.

Incident Update

11/17/14:
VA Police are investigating, but at this time, it is unknown who left or how long the list was in the waiting room. The manager, supervisor and clerk have been interviewed. There were security cameras in the waiting room, but they were not functioning. The documents found were dated 10/24/14 and contain the name, full SSN, appointment desired date, specialty clinic, site current status, originating date and wait list type for 1,094 Veterans.

11/18/14:
The DBCT has determined that this is a data breach. It is a HITECH Act data breach, will require offers of credit protection services for all 1,094 Veterans involved, and will require a press release.

12/01/14:
After duplicates have been removed, the total number of individuals involved is 1,081.

12/09/14:
The press release and credit monitoring letter have been approved and sent back to the facility.

DBCT Decision Date: 11/18/2014

DBCT

11/18/14:
The DBCT determined that this is a data breach based on the unknown amount of time that the documents were out of a VA secured environment, and the information included in the documents.

Security Privacy Ticket Number:	PSETS0000111691
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VHA CMOP Dallas, TX
Date Opened:	11/17/2014
Date Closed:	12/8/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0613407
Date US-CERT Notified:	11/17/2014
US-CERT Case Number:	INC000000418237
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 El Paso VA Medical Center and a replacement has been requested for Patient B. The Dallas 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

11/17/14:
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 11/17/14, 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 9 Mis-Mailed CMOP incidents out of 6,316,302 total packages (8,964,105 total prescriptions) mailed out for this reporting period. Because of repetition, the other 8 are not included in this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number:	PSETS0000111765
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VBA Atlanta, GA
Date Opened:	11/18/2014
Date Closed:	11/25/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0613479
Date US-CERT Notified:	11/18/2014
US-CERT Case Number:	INC000000418637
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	1
No. of Loss Notifications:	
DBCT Category:	Mismailed

Incident Summary

Veteran A contacted the Atlanta Regional Office stating that he had received documents belonging to Veteran B attached to his letter. The documents contained Veteran B's name, social security number, and address.

Incident Update

11/18/14:
The Incident Resolution Service Team has determined that Veteran B will be sent a letter offering credit protection services.

Resolution

The employee was verbally counseled by his Supervisor on November 20, 2014. When the letter was prepared, the employee unintentionally attached both letters together. Veteran A and Veteran B's addresses were verified for future mailing. All forms were filed in the correct claim folder. The letter was resent to the correct Veteran and data was corrected in all IT systems.

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 102 Mis-Mailed incidents this reporting period. Because of repetition, the other 101 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:	PSETS0000112074
Incident Type:	Missing/Stolen Equipment
Organization:	VISN 04 Pittsburgh, PA
Date Opened:	11/25/2014
Date Closed:	12/5/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0613811
Date US-CERT Notified:	11/25/2014
US-CERT Case Number:	INC000000420502
US-CERT Category:	Category 1 - Unauthorized Access
No. of Credit Monitoring:	
No. of Loss Notifications:	
DBCT Category:	Unencrypted iPad Missing

Incident Summary

An iPad issued to a VA RN has been lost. The employee has not seen the device for several months. This device is part of the VHA Mobile Device Deployment. It contained no sensitive information since it was never used by the employee.

Incident Update

12/01/14:
The Incident Resolution Service Team has determined that no data breach has occurred. The information security officer stated that the device contained no patient data.

Resolution

Employee has left VA service.

DBCT Decision Date:

DBCT

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