Information Security
Monthly Activity Report*

INFOCON LEVEL
CRITICAL
SEVERE
ELEVATED
GUARDED
NORMAL

June 2015

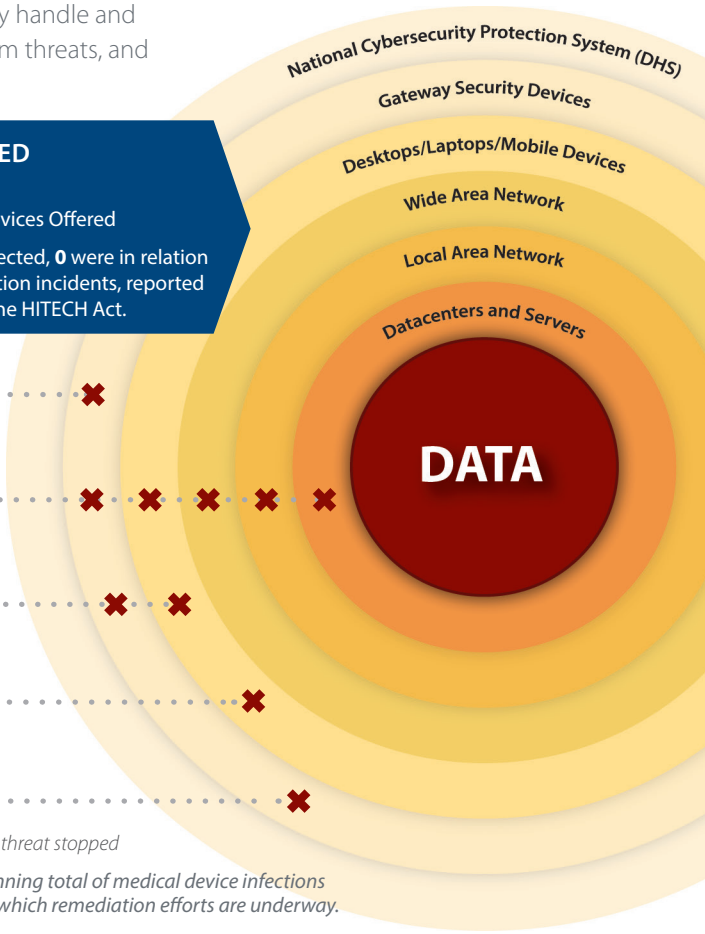
VA uses a defense-in-depth approach to information security to protect the data we hold on Veterans. While the defense-in-depth approach protects from inbound threats and contains other data exposing incidents, VA relies on employees to protect Veteran information they handle and transmit. This graphic 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)
389,303,055

Malware (Blocked/Contained)
680,233,603

Suspicious/Malicious Emails (Blocked)
103,106,116

Infected Medical Devices (Contained)**
3

Outgoing Unencrypted Emails
93 Associated Privacy/Security Events
15,059 Total Emails Blocked

✖ = *threat stopped*

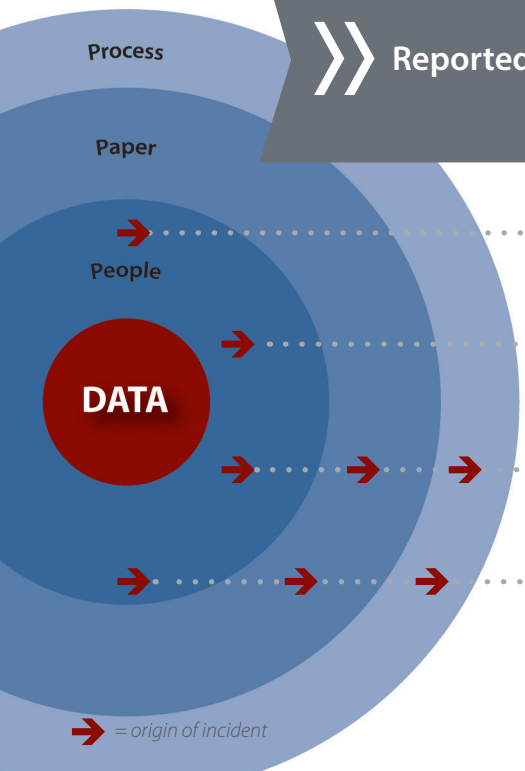
** *Running total of medical device infections for which remediation efforts are underway.*

Reported Events

2,076 VETERANS AFFECTED

543 Notifications
1,533 Credit Protection Services Offered

Of the total # of Veterans affected, 935 were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



→ = *origin of incident*

Lost and Stolen Device Incidents
43

Lost PIV Cards
143

Mishandled Incidents
104

Mis-mailed Incidents
161 Paper Mis-mailings
22 Pharmacy-item Mis-mailings
out of **7,313,422** 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

June 1-30, 2015

Security Privacy Ticket Number:	PSETS0000120314
DBCT Category:	Mishandling
Organization:	VISN 15 Columbia, MO
Date Opened:	6/3/2015
Date Closed:	6/9/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0621724
Date US-CERT Notified:	6/3/2015
US-CERT Case Number:	INC000010001239
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	193
No. of Loss Notifications:	

Incident Summary

A Medical Support Assistant (MSA) reporting for duty found a 6 page list on her desk which is at the check-in station for the Specialty Care clinic. The list was face up on the desk with names and SSNs highlighted for each of the 191 patients. The MSA reported finding the list immediately and the Privacy Officer (PO) picked it up from her.

Incident Update

06/03/15:
The Incident Resolution Service Team has determined that 191 Veterans will be sent letters offering credit protection services.

06/05/15:
On further review the final count is 193.

Resolution

The Privacy Officer provided re-education to the staff member responsible for the incident. Credit monitoring letters were mailed to all names on the list. The Specialty Care Service Chief to follow up regarding further actions with the staff member.

DBCT Decision Date:

DBCT

This incident remains on this report due to the number of affected individuals.

Security Privacy Ticket Number:	PSETS0000120416
DBCT Category:	IT Equipment Inventory
Organization:	VISN 03 Montrose, NY
Date Opened:	6/4/2015
Date Closed:	6/8/2015
Date of Initial DBCT Review:	6/9/2015
VA-NSOC Incident Number:	VANSOC0621823
Date US-CERT Notified:	6/4/2015
US-CERT Case Number:	INC000010001856
US-CERT Category:	Category 1 - Unauthorized Access
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

A Report of Survey (ROS) was issued for FY 2015 for Hudson Valley HealthCare System (HVHCS) Information Technology Inventory which identified 1 Laptop, 2 Cameras, 2 TVs, 67 Cell Phones, 3 BlackBerry devices, 2 USB, 18 PCs, 72 Monitors, 2 Tandberg, 5 Servers, 2 Switches, and 18 Printers that cannot be located. The PCs and Servers did not contain hard drives, as the hard drives were disposed of separately.

Incident Update

06/06/15:
The ISO reports that after working with the IT staff it has been determined that the laptop also had its hard drive removed.

Resolution

The ROS and loss was a known issue due to inventory issues and excessed equipment. All equipment that has the ability to store data had been previously sanitized, kill signals were sent to BlackBerry devices, and hard dives were removed and disposed of according to VA guidelines. In response to an Incident Resolution Service Team inquiry, the laptop was discovered soon after the ROS was completed. The laptop had been on a turn-in request and the hard drive was removed at that time.

DBCT Decision Date: 06/09/2015

DBCT

06/09/15:
This incident was discussed by the Data Breach Core Team (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 2 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other IT Equipment Inventory Incident is not included in this report.

Security Privacy Ticket Number:	PSETS0000120460
DBCT Category:	CMOP Mismailed
Organization:	VHA CMOP Hines, IL
Date Opened:	6/5/2015
Date Closed:	6/26/2015
Date of Initial DBCT Review:	6/9/2015
VA-NSOC Incident Number:	VANSOC0621863
Date US-CERT Notified:	6/5/2015
US-CERT Case Number:	INC000010002163
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	
No. of Loss Notifications:	62

Incident Summary

Sixty two (62) Patients-A received a Medline Industries medical supply intended for sixty two (62) Patients-B. Sixty two (62) of Patient-Bs' name, address, and type of medical supply were compromised. Patients-A reported the incident to their medical centers and a replacement has been requested for Patients-B. Great Lakes Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a Medline packing error. On 04/13/15, Medline Industries installed a new automated system for applying shipping labels to CMOP packages which did not work properly therefore causing these mismailings. The packing errors have been reported to Medline for investigation and corrective action.

Total # of Affected Patients: 62

Incident Update

06/05/15:
The Incident Resolution Service Team has determined that 62 Veterans will be sent a notification letter.

Resolution

On 6/5/15, the packing errors were reported to Medline for investigation and corrective action.

DBCT Decision Date:

DBCT

06/09/15:
This was brought to the attention of the DBCT because there were multiple incidents regarding this breach. At this point there are 401 individuals involved.

06/16/15:
The total is now 456 individuals for all incidents regarding this Medline issue.

06/23/15:
The total is now 481 individuals for all incidents regarding this Medline issue. The DBCT determined that these should be considered separate incidents based on the facilities.

Security Privacy Ticket Number:	PSETS0000120461
DBCT Category:	CMOP Mismailed
Organization:	VHA CMOP Charleston, SC
Date Opened:	6/5/2015
Date Closed:	6/19/2015
Date of Initial DBCT Review:	6/9/2015
VA-NSOC Incident Number:	VANSOC0621864
Date US-CERT Notified:	6/5/2015
US-CERT Case Number:	INC000010002171
US-CERT Category:	Category 4- Improper Usage
No. of Credit Monitoring:	
No. of Loss Notifications:	121

Incident Summary

One-hundred twenty-one (121) Patients-A received a Medline Industries medical supply intended for one-hundred twenty-one (121) Patients-B. One-hundred twenty-one (121) of Patient-Bs' name, address, and type of medical supply was compromised. Patients-A reported the incident to their medical centers and a replacement has been requested for Patients-B. Charleston Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a Medline packing error. On 04/13/15, Medline Industries installed a new automated system for applying shipping labels to CMOP packages which did not work properly therefore causing these mismailings. The packing errors have been reported to Medline for investigation and corrective action.

Total # of Affected Patients: 121

Incident Update

06/05/15:
The Incident Resolution Service Team has determined that 121 Veterans will be sent notification letters.

Resolution

On 6/5/15, the packing errors were reported to Medline for investigation and corrective action.

DBCT Decision Date: 06/09/2015

DBCT

No DBCT decision required. This incident is left on this report due to the number of affected individuals. DBCT information regarding this is in PSETS 120640.

There were a total of 22 Mismailed CMOP incidents out of 7,313,422 total packages (10,438,688 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:	PSETS0000120554
DBCT Category:	Mismailed
Organization:	VBA Togus, ME
Date Opened:	6/9/2015
Date Closed:	6/11/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0621961
Date US-CERT Notified:	6/9/2015
US-CERT Case Number:	INC000010003069
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	1
No. of Loss Notifications:	

Incident Summary

Veteran A received information pertaining to Veteran B in the mail. The information included Veteran B's name, SSN, Power of Attorney (POA), branch of service and service dates. Veteran A returned the information he received in error via mail. The improperly disclosed information is back in VA custody.

Incident Update

06/09/15:
The Incident Resolution Service Team has determined that Veteran B will be sent a letter offering credit protection services due to full SSN being disclosed.

Resolution

The employee responsible for the improper disclosure received counseling on the incident. A refresher training course on PII protection was also recommended.

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 161 Mis-Mailed incidents this reporting period. Because of repetition, the other 160 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:	PSETS0000120909
DBCT Category:	Mishandling
Organization:	VISN 20 Anchorage, AK
Date Opened:	6/15/2015
Date Closed:	
Date of Initial DBCT Review:	6/23/2015
VA-NSOC Incident Number:	VANSOC0622325
Date US-CERT Notified:	6/16/2015
US-CERT Case Number:	INC000010005242
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	1008
No. of Loss Notifications:	

Incident Summary

On Wednesday, 06/10/15, the Salt Lake City Regional Office (RO) was notified of an issue involving personally identifiable information (PII). The Wounded Warrior Program Office in Settle received a box from a Veteran in Anchorage AK (assuming it was the Veteran's records). A Veteran had previously gone to the Anchorage RO and asked for a copy of her VA file and apparently left with a box containing PII of an unknown origin, and not her records. Upon receiving the box, the Seattle RO opened and reviewed the contents, what appeared to be primarily Human resources (HR) and payroll related, to include names and SSNs for VA employees, but other Veteran data was also present (name and SSNs).

Incident Summary (continued)

Update as of 3:45 PM: The Anchorage RO Privacy Officer (PO) contacted the Veteran and received the following explanation;

- The Veteran reported that in mid-April of this year she brought her records to the ANC VHA HR department, where an HR representative agreed to take the records and make copies. She left her originals to be copied.
- Several weeks later, she returned to VHA HR department and spoke to the HR receptionist about getting the documents back. The receptionist located the box in question and gave it to the Veteran, indicating those were the records she was asking for.
- Several days later, the Veteran decided she needed to remove her originals from the box and forward the copies to her Veterans Service Organizations (VSO) (Seattle area).
- She opened the box and discovered the documents were not hers.
- The Veteran told the PO that she panicked and then mailed them to her VSO, thinking he would know what to do with them.

It appears the box contains miscellaneous HR forms such as VA Form 5-97 re: Notice of Pending Personnel Action forms and Finance Activity Forms from Austin Data Processing Center (DPC) with Station 463 employees listed. The Seattle RO is sending via FEDEX the box of records to the Anchorage RO to return the box to VHA HR for their follow-up action.

Incident Update

06/23/15:
Although it was originally reported that Veteran data was in the box, it was investigated that it was only employee data was in the box, though some of these employees were also Veterans. It was not Veteran's PHI. The Data Breach Core Team determined this was a data breach, and that all employees will be offered credit protection services. Currently the number is 1,008, but some duplicates are included in that number.

DBCT Decision Date: 06/23/2015

DBCT

06/23/15:
The DBCT concurred that this is a data breach.

Security Privacy Ticket Number:	PSETS0000121109
DBCT Category:	Unencrypted iPad Stolen
Organization:	VISN 07 Augusta, GA
Date Opened:	6/19/2015
Date Closed:	7/8/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0622493
Date US-CERT Notified:	6/19/2015
US-CERT Case Number:	INC000010006428
US-CERT Category:	Category 1 - Unauthorized Access
No. of Credit Monitoring:	
No. of Loss Notifications:	

Incident Summary

An employee noticed that after she moved between offices, her IPAD was missing.

MANUFACTURER: VERIZON
MODEL: MD543LL/A
SN: F7NML5JPF19M

Incident Update

06/25/15:
The Incident Resolution Service Team has determined that no data breach has occurred. There was no VA data stored on the device.

Resolution

The employee reported that she had not logged into the device since it was issued. The employee has received administrative counseling for the missing device. The device has not been recovered.

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:	PSETS0000121413
DBCT Category:	Mishandling
Organization:	VISN 18 Albuquerque, NM
Date Opened:	6/26/2015
Date Closed:	7/13/2015
Date of Initial DBCT Review:	6/30/2015
VA-NSOC Incident Number:	VANSOC0622823
Date US-CERT Notified:	6/26/2015
US-CERT Case Number:	INC000010008467
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	73
No. of Loss Notifications:	

Incident Summary

Veteran A returned a list to the facility Operation Enduring Freedom/Operation Iraqi Freedom (OEF-OIF) Office and explained to the manager that following a recent visit "a couple of days earlier" to OEF-OIF Office, the list was found in the paperwork he had picked up from OEF-OIF Office and had taken home. The original list was returned to OEF-OIF manager who immediately reported privacy violation and turned in list to Privacy Officer (PO). Fact-finding initiated to determine circumstances and address necessary corrective action. The printed list contained full names and full SSN with appointment date/time for 73 Veterans and noted status of note entry for OEF/OIF case management.

Incident Update

06/26/15:
The Incident Resolution Service Team has determined that 73 Veterans will be sent letters offering credit protection services, as their names, full SSNs and appointment information were disclosed inappropriately.

Resolution

This error has been remediated by re-training and conducting heightened awareness for responsible staff and reminding staff of the requirement for securing of all Veteran information and assuring confidential handling of this information at all times and by assuring appropriate individual accountability for the involved staff via appropriate HR action. Additionally, the facility has undertaken an immediate revision of internal processes in the handling of this information to include eliminating the inclusion of the full social security number on such work lists and replacing with just the last 4 digits of the social security number. The work process in this area was reviewed and revisions in this area addressed the responsibility for all OEF/OIF/OND Program Staff to assure that patient privacy is maintained by securing and protecting individually identifying Protected Health Information and by processing such working lists electronically only, with no further printing of such information and by assuring that computer work stations are closed when the employee is away from their work station. The above remediation and corrective actions have been undertaken in order to prevent such incidents from happening again. Letters of notification and offering credit monitoring prepared for each affected Veteran for immediate mail-out.

DBCT Decision Date: 06/30/2015

DBCT

06/30/15:
The DBCT concurred with the IRST decision.

Security Privacy Ticket Number:	PSETS0000121564
DBCT Category:	Mishandling
Organization:	VISN 06 Durham, NC
Date Opened:	6/30/2015
Date Closed:	7/7/2015
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0622950
Date US-CERT Notified:	6/30/2015
US-CERT Case Number:	INC000010009505
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	
No. of Loss Notifications:	1

Incident Summary

Veteran A and B have the same last name, a similar first name and the same last four digits of the SSN. A VA employee gave Veteran A's appointment list to Veteran B in error.

Incident Update

06/30/15:
The Incident Resolution Service Team has determined that Veteran A will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

Education provided to the responsible employee and the Veteran's chart was flagged as sensitive to prevent future errors.

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 104 Mis-Handling incidents this reporting period. Because of repetition, the other 103 are not included in this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.