Information Security
Monthly Activity Report*

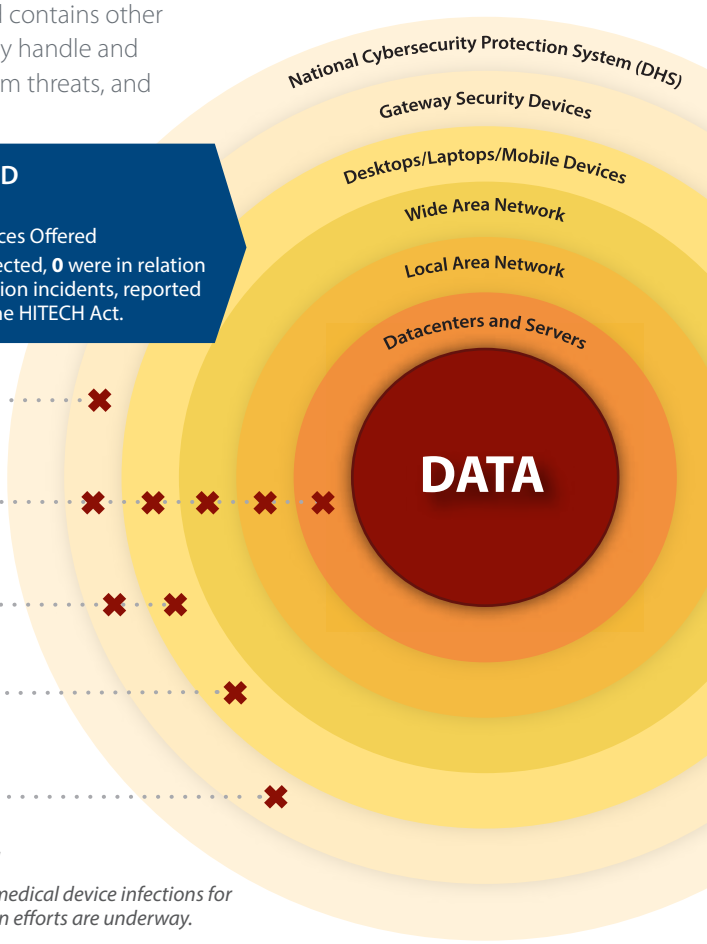
October 2014

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) **12,148,205**
- Malware (Blocked/Contained) **206,564,180**
- Suspicious/Malicious Emails (Blocked) **71,598,834**
- Infected Medical Devices (Contained)** **27**
- Outgoing Unencrypted Emails (Blocked) **96**

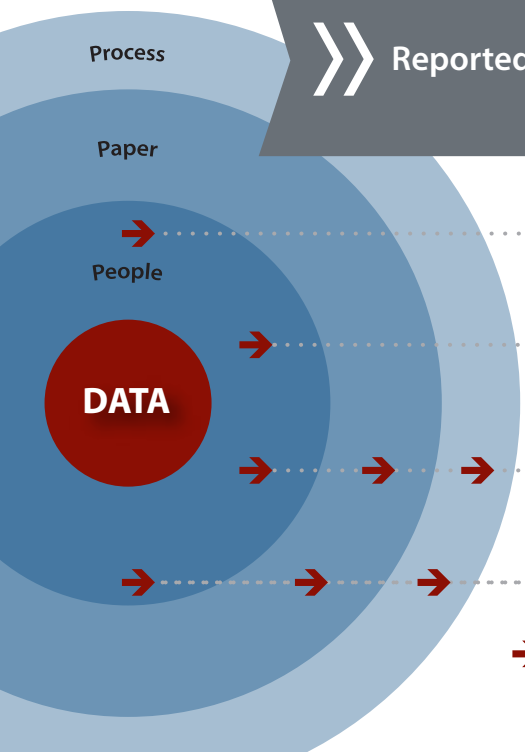
✖ = threat stopped

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

Reported Events

765 VETERANS AFFECTED
- **229** Notifications
- **536** Credit Protection Services Offered

Of the total # of Veterans affected, **640** were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



- Lost and Stolen Devices **52**
- Lost PIV Cards **131**
- Mishandled Incidents **128**
- Mis-mailed Incidents **146**

→ = 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 on Data Incidents

October 1 - 31, 2014

Security Privacy Ticket Number:	PSETS0000109871
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 06 Salem, VA
Date Opened:	10/1/2014
Date Closed:	10/7/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0611676
Date US-CERT Notified:	10/1/2014
US-CERT Case Number:	INC000000405011
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	1
No. of Loss Notifications:	
DBCT Category:	Mismailed

Incident Summary

A medication list, including the Veteran's name, date of birth and full SSN, was sent by a clinic to the incorrect Veteran.

Incident Update

10/01/14:
The Incident Resolution Service Team has determined that the Veteran whose information was disclosed will be sent a letter offering credit protection services.

Resolution

The redacted letter has been uploaded and the employee has been cautioned to be more careful. The document was returned by the Veteran who received it in error.

DBCT Decision Date: N/A

DBCT

No DBCT decision is required. This is informational for Mis-Mailed incidents and is the representative ticket. There were a total of 155 Mis-Mailed incidents this reporting period. Because of repetition, the other 154 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:	PSETS0000109883
Incident Type:	Unauthorized Electronic Access
Organization:	VISN 17 Dallas, TX
Date Opened:	10/1/2014
Date Closed:	
Date of Initial DBCT Review:	10/7/2014
VA-NSOC Incident Number:	VANSOC0611685
Date US-CERT Notified:	10/1/2014
US-CERT Case Number:	INC000000405071
US-CERT Category:	Category 4- Improper Usage
No. of Credit Monitoring:	90
No. of Loss Notifications:	
DBCT Category:	Mishandling

Incident Summary

The Privacy Officer (PO) received a report that at least 12 of the employees in Human Resources Management Service (HRMS) accessed electronic official personnel folders (eOPFs) and USA Staffing to review the files of at least 90 individuals, some of which are not employees. The individuals did so without a need to know for their official duties.

Incident Update

10/01/14:
An access report was run and identified who accessed the record, when, and at what time. It was determined from this report that the employees did not have a working need to do so. The supervisors of the employees were interviewed, and from those interviews it was determined that the records should not have been accessed by the employees.

10/17/14:
The Privacy Officer (PO) was informed this case was referred to OIG, but was not accepted. OIG suggested that the facility proceed as usual administratively.

10/27/14:
HR informed the PO of the following regarding why the employees accessed the records inappropriately and their intent. Some accessed the records for better preparation, and some for curiosity. Also, the one person who looked at management eOPFs may have done it maliciously to share information with the Union.

10/28/14:
The Incident Resolution Service team recommended that everyone whose record was accessed inappropriately will receive a letter offering credit protection services.

DBCT Decision Date: 10/28/2014

DBCT

10/07/14:
The incident was first presented to DBCT.

10/28/14:
The DBCT concurred with the Incident Resolution Service Team recommendation to provide credit protection services for everyone whose record was inappropriately accessed.

Security Privacy Ticket Number:	PSETS0000110005
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Louisville, KY
Date Opened:	10/3/2014
Date Closed:	
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0611800
Date US-CERT Notified:	10/3/2014
US-CERT Case Number:	INC000000405961
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	1
No. of Loss Notifications:	
DBCT Category:	Mishandling

Incident Summary

Veteran A received information at his appointment on 09/16/14. When going through the information he was given at that appointment, he discovered that Veteran B's medication list was included in his information. He immediately returned the medication list of the other Veteran to the Fort Knox clinic very concerned that the other Veteran would not get his medication. He was assured that the other Veteran already received his medication. He was satisfied after being told this and left.

Incident Update

10/03/14:
The Incident Resolution Service Team has determined that Veteran B will be sent a letter offering credit protection services. The information disclosed included Veteran B's name, date of birth, SSN, and medications.

Resolution

The Veteran who received the incorrect information immediately reported and returned the information to the clinic. When speaking of the other Veteran, he called him by the wrong name, so it was obvious that he did not pay attention to the information that was not his. The Privacy Officer spoke with the Nurse Manager of the clinic, who was the one who reported this incident and she indicated that she spoke with the Veteran who turned the information in and he was satisfied when he left. She has also spoken with her staff and stressed that they have to make sure and look at the information being handed to the Veterans to ensure that it is only their information being given and does included someone else's information. She went on to tell the PO that they do not have enough printers and this is why this happened. I indicated to the Nurse Manager that even though there are not enough printers does not negate the responsibility of staff to check the information being given to the Veterans.

DBCT Decision Date: N/A

DBCT

No DBCT decision is required. This is informational for Mis-Handling incidents and is the representative ticket. There were a total of 135 Mis-Handling incidents this reporting period. Because of repetition, the other 134 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:	PSETS0000110093
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 21 Honolulu, HI
Date Opened:	10/6/2014
Date Closed:	10/20/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0611886
Date US-CERT Notified:	10/6/2014
US-CERT Case Number:	INC000000406646
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	55
No. of Loss Notifications:	
DBCT Category:	Mishandling

Incident Summary

A Community Based Outpatient Clinic (CBOC) had a table at the Maui County Fair and materials were laid out to educate Veterans on services. When an employee had returned to the booth the following morning, she had found PII/PHI reports from VistA that contained the full name and social security numbers of Veterans on the bottom of one of the magazine holders that they had brought with them.

Incident Update

10/06/14:
The Incident Resolution Service Team has determined that fifty-five Veterans will be sent letters offering credit protection services.

Resolution

Privacy/Information Security training has been provided for staff. The Privacy Officer will be traveling to the CBOC to provide an in-service as soon as possible.

DBCT Decision Date: N/A

DBCT

No DBCT decision was required. This stays on the report due to the number of individuals affected.

Security Privacy Ticket Number:	PSETS0000110330
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VHA CMOP Hines, IL
Date Opened:	10/13/2014
Date Closed:	10/23/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0612105
Date US-CERT Notified:	10/13/2014
US-CERT Case Number:	INC000000408361
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, address, and type of medication were compromised. Patient A reported the incident to the medical center and a replacement has been requested for Patient B. 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

10/14/14:
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

The CMOP employee was counseled and retrained in proper packing procedures.

DBCT Decision Date: N/A

DBCT

No DBCT decision is required. This is informational for Mis-Mailed CMOP incidents and is the representative ticket. There were a total of 6 Mis-Mailed CMOP incidents out of 7,306,531 total packages (10,517,751 total prescriptions) mailed out for this reporting period. Because of repetition, the other 5 are not included in this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number:	PSETS0000110385
Incident Type:	Missing/Stolen Equipment
Organization:	VISN 17 Temple, TX
Date Opened:	10/14/2014
Date Closed:	10/16/2014
Date of Initial DBCT Review:	N/A
VA-NSOC Incident Number:	VANSOC0612156
Date US-CERT Notified:	10/14/2014
US-CERT Case Number:	INC000000408756
US-CERT Category:	Category 1 - Unauthorized Access
No. of Credit Monitoring:	
No. of Loss Notifications:	
DBCT Category:	IT Equipment Inventory

Incident Summary

Following an IT inventory, the ISO was informed of unaccounted for equipment from the IT Equipment Inventory Listing. This is a preliminary report of current findings of five laptops and five computers and three thumb drives unaccounted for. Updates to this finding are ongoing and the ISO will continue to monitor and respond to this ticket with updated information as provided from IT specialists, police, and other facility staff as they continue to search for equipment. A report of Survey (ROS) and VA Police Report for this equipment are being completed.

Incident Update

10/15/14:
Per the Information Security Officer, all the devices were encrypted and IT policies prevented any information from being stored locally on hard drives. The systems have been off the VA network for long enough that the computer certificates have expired, so they will not be able to connect to the VA network. The ISO will work with the Region 2 Client Tech team to test setting up a way to do a remote device wipe of the equipment.

10/16/14:
One thumb drive has been located and will be sanitized per VA policy.

Resolution

One of the PCs did have its hard drive (9LS6D63H) removed and sanitized by Intelligent Decisions. This system should have been turned in, but the turn-in paperwork cannot be located at this time. OI&T is still searching for systems and will notify the ISO and facility leadership if/when the devices are found. ISO will provide additional feedback, input, updates and information as it becomes available.

DBCT Decision Date: N/A

DBCT

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:	PSETS0000110435
Incident Type:	Mishandled/ Misused Physical or Verbal Information
Organization:	VISN 09 Mountain Home, TN
Date Opened:	10/15/2014
Date Closed:	
Date of Initial DBCT Review:	10/21/2014
VA-NSOC Incident Number:	VANSOC0612204
Date US-CERT Notified:	10/15/2014
US-CERT Case Number:	INC000000409083
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	106
No. of Loss Notifications:	
DBCT Category:	Mishandling

Incident Summary

A housekeeper was sorting through the paper recycling bins in the parking lot and found a stack of papers containing patient names, SSNs, dates of birth and a list of medications.

Incident Update

10/17/14:
Thee paper recycling bins were in the parking lot because that is where city employees pick up and empty them. The housekeeping staff roll the recycle bins out the back dock once a week to be emptied by the city's recycling staff. The facility has a contract with the city to pick these up. This particular housekeeper opened one of the other bins and noticed the paper.

The bins are usually located throughout the facility and are used for recycling telephone books, and various papers that do not contain personally identifiable information (PII). There are no cameras on the recycling bin when the PII was found. The Privacy Officer (PO) is sorting through the papers in an effort to identify where they came from. The PO has 109 pages, and she is going to sort according to provider, pharmacist, medication and dates. She is sure it was one of the Pharmacists who inappropriately discarded the papers. Pharmacy says they can probably figure it out once the PO can get the sort narrowed down by date.

10/21/14:
The Pharmacy is unsure how the papers from the narcotics vault ended up outside the shred box, but they have decided to assign one tech to empty sensitive papers in the shred box. They have asked for a shred box for the vault either to go into the vault or just outside the vault door.

It is hard to determine when or where the 109 pages from July have been or why they were just discovered last week. Normally the vault staff put the sensitive papers in the shred box on average once a week. They often catch the shred worker as he comes by and dumps directly into his container. It could have been dropped by the shred company on the way to their truck. He does not keep the container closed in the Pharmacy area when he makes a pick up. He does not always empty every bin in the pharmacy each week. The Pharmacy has several staff members, residents, and students in and out of the pharmacy that could potentially put paperwork in a recycle paper bin or trash in error in times of heavy workload.

10/23/14:
There was information on 106 different Veterans, including full name, patient ID number, date of birth, gender, height, weight, name of medication, prescription number, date filled, total quantity, quantity dispensed, how many and how often to take, provider's name and DEA number, clinic name and date of visit, and the name of the Pharmacist who filled it.

The bins were already outside when the housekeeper found it. The area is accessible to the public. The bin was inside Pharmacy. Exactly when it was taken to the back dock is unknown. The housekeeper opened the bin that was outside, to see if the city had been by and emptied them, so he could swap full ones out with the empty ones, and discovered that the previous placed bins had not been emptied and noticed the documents containing PII. The city is supposed to come by once a week, on Wednesday. That is also why the housekeeper was checking on that Wednesday to determine if he was ahead of or behind the city's visit. The PO has confirmation that they picked up on 10/01/14, but no true validation for 10/08/14. It is unknown exactly what day the bin went outside and it could have been as early as 10/01/14. It was removed on 10/15/14, so it could have been there two weeks.

10/28/14:
The Incident Resolution Service Team determined that the 106 Veterans will receive a letter offering credit protection services.

DBCT Decision Date: 10/28/2014

DBCT

10/21/14:
The incident was presented to the DBCT. DBCT inquires about what data elements were exposed and what the final count is.

10/28/14:
The DBCT concurred with the IRST determination.

Security Privacy Ticket Number:	PSETS0000110611
Incident Type:	Missing/Stolen Equipment
Organization:	VISN 02 Albany, NY
Date Opened:	10/20/2014
Date Closed:	11/3/2014
Date of Initial DBCT Review:	10/21/2014
VA-NSOC Incident Number:	VANSOC0612375
Date US-CERT Notified:	10/20/2014
US-CERT Case Number:	INC000000410360
US-CERT Category:	Category 6 - Investigation
No. of Credit Monitoring:	
No. of Loss Notifications:	
DBCT Category:	Unencrypted Desktop Stolen

Incident Summary

A Platelet Aggregation workstation (Bio Data Corp) was reported missing by the supervisory medical technologist. This device (Dell computer) was not connected to the VA network. The component of the device which has been reported missing is the CPU. The information captured by the device is patient last name and graph of numbers. The ISO is working with the CIO to determine if device was encrypted. This has been reported to the VA police

Incident Update

10/21/14:
The Biomedical Engineer has confirmed that this device is a medical device and it is not encrypted. The ISO is still waiting for the police report number and will respond back when it is available.

10/27/14:
The device has not been found and was never on the VA network. The device had five patients' last names and a graph of numbers.

11/10/14:
The DBCT determined this to be low risk of compromise based on the type of information involved.

Resolution

Lab managers were advised to secure computers that are not used routinely and store patient information.

DBCT Decision Date: 11/10/2014

DBCT

10/29/14:
Only a trained Medical Technologist would be able to understand the raw data. The Medical Technologist manually enters the data into CPRS.

11/10/14:
The DBCT determined this to be a low risk of compromise based on the type of data involved, and because the hard copy was not missing.