Information Security
Monthly Activity Report*

INFOCON LEVEL
CRITICAL
SEVERE
ELEVATED
GUARDED
NORMAL

September 2015

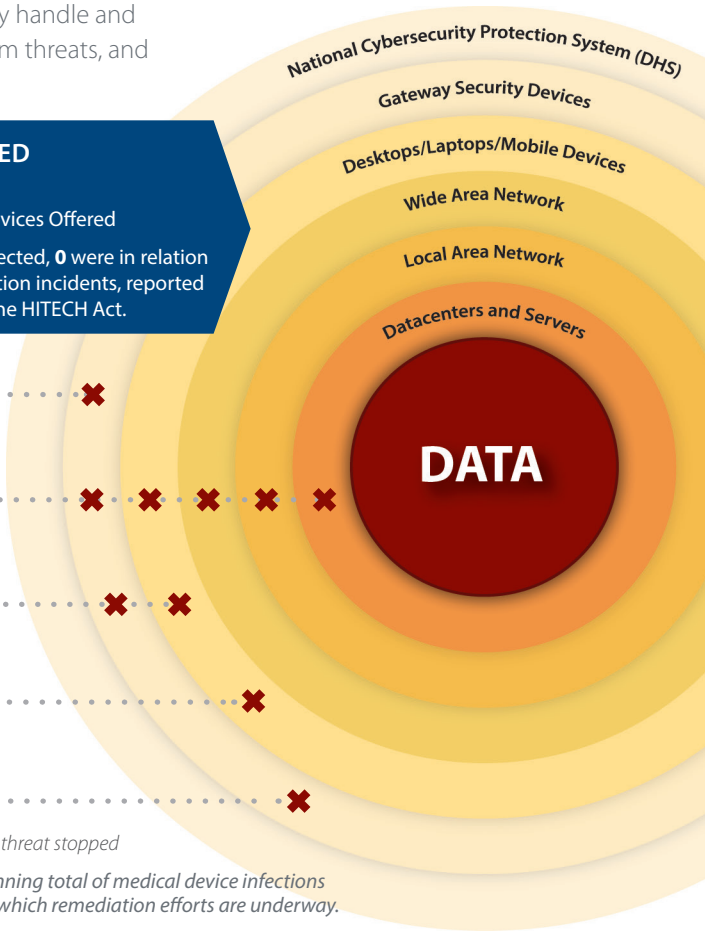
VA uses a defense-in-depth approach to information security to protect the data we hold on Veterans. While the defense-in-depth approach protects from inbound threats and contains other data exposing incidents, VA relies on employees to protect Veteran information they handle and transmit. This graphic 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)
200,384,851

Malware (Blocked/Contained)
540,486,893

Suspicious/Malicious Emails (Blocked)
94,664,365

Infected Medical Devices (Contained)**
1

Outgoing Unencrypted Emails
64 Associated Privacy/Security Events
15,847 Total Emails Blocked

✖ = *threat stopped*

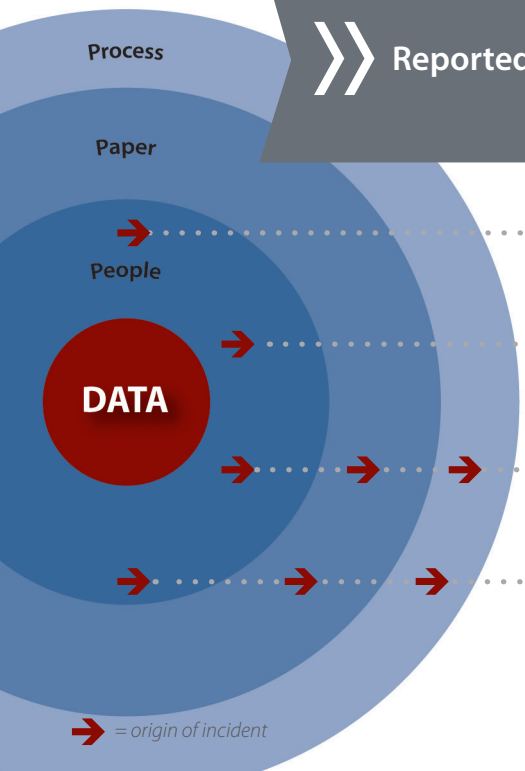
** *Running total of medical device infections for which remediation efforts are underway.*

Reported Events

1,135 VETERANS AFFECTED

- **739** Notifications
- **396** Credit Protection Services Offered

Of the total # of Veterans affected, **930** 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
64

Lost PIV Cards
134

Mishandled Incidents
115

Mis-mailed Incidents
137 Paper Mis-mailings
5 Pharmacy-item Mis-mailings
out of **7,151,070** 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 on Data Incidents

September 1 – 30, 2015

Security Privacy Ticket Number: PSETS0000124068

DBCT Category: Mismailed

Organization: VISN 09
Lexington, KY

Date Opened: 9/1/2015

Date Closed: 9/2/2015

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

Veteran A received Veteran B's appointment letter and his lab results. Both letters have been returned.

Incident Update

09/01/15:
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.

Resolution

The staff involved has been educated on proper handling of PHI.

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 137 Mis-Mailed incidents this reporting period. Because of repetition, the other 136 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: PSETS0000124070

DBCT Category: Mishandling

Organization: VISN 07
Montgomery, AL

Date Opened: 9/1/2015

Date Closed: 9/22/2015

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

An employee posted on a Veteran's online obituary "It is with deepest regret to hear of Mr. XX passing, he left an impression on the mental health department and staff with smiles and memories."

Incident Update

09/01/15:
The Incident Resolution Service Team has determined that the Veteran's Next of Kin will be sent a notification letter.

Resolution

The employee was counseled on the inappropriateness of her comments. The employee acknowledged her understanding of privacy concerns.

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 115 Mis-Handling incidents this reporting period. Because of repetition, the other 114 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: PSETS0000124093

DBCT Category: Mishandling

Organization: VISN 21
Palo Alto, CA

Date Opened: 9/1/2015

Date Closed: 9/11/2015

Date of Initial DBCT Review: 9/8/2015

No. of Credit Monitoring:

No. of Loss Notifications: 50

Incident Summary

A Housing and Urban Development-Veterans Affairs Supported Housing (HUD-VASH) Case Manager's briefcase was stolen from a government vehicle. The briefcase was not lockable and contained a list of 50 Veterans' names, last 4 digits of their Social Security Numbers, telephone numbers and home addresses. The Santa Cruz County Police, VA Police and VAPAHCS Privacy Officers (PO) have been notified.

Incident Update

09/03/15:
The Incident Resolution Service Team has determined that 50 Veteran will be sent a general notification letter.

Resolution

Notification letters were mailed on September 11, 2015. The employees within the service will be retrained on safeguarding sensitive information and HIPPA bags will be issued to the VASH team.

DBCT Decision Date: 9/8/2015

DBCT: This incident was briefed to the Data Breach Core Team for awareness, due to the number of Veterans affected. The Data Breach Core Team concurred with the decision of the Incident Resolution Service Team.

Security Privacy Ticket Number: PSETS0000124185

DBCT Category: IT Equipment Inventory

Organization: VISN 12
Milwaukee, WI

Date Opened: 9/2/2015

Date Closed: 9/28/2015

Date of Initial DBCT Review: 9/8/2015

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

A local IT inventory was conducted and IT staff is not able to account for various pieces of IT equipment.
It is unknown if the equipment contained sensitive information, however all IT assets are encrypted. There is no evidence that these assets have been stolen.

VA Police have conducted their investigation and a report of Surveys has been initiated.

Incident Update

09/03/15:
The Incident Resolution Service Team has determined that no data breach has occurred; this is being briefed to the DBCT for situational awareness due to it being missing equipment associated with an IT Inventory. The investigation could not confirm if any of the items actually contained any SPI, however all IT assets that were noted as missing were confirmed to have been encrypted.

Resolution

VA Police have already conducted their investigation. A report of Survey has already been completed. The Director and VISN leadership have been notified.

DBCT Decision Date: 09/08/2015

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 14 IT Equipment Inventory Incidents this reporting period.

Security Privacy Ticket Number: PSETS0000124286

DBCT Category: Mishandling

Organization: VISN 08
Bay Pines, FL

Date Opened: 9/4/2015

Date Closed:

Date of Initial DBCT Review: 10/6/2015

No. of Credit Monitoring:

No. of Loss Notifications: 58

Incident Summary

While conducting an internal inspection regarding unauthorized access, it was discovered that Employee A may have inappropriately accessed the electronic medical records of approximately 65 other VA employees.

Incident Update

09/18/15:
The employee has not returned to work since being informed that there will be an investigation of this access.

09/30/15:
The employee has had two HIPAA violations in the past and has not returned to work. Human Resources has asked the Privacy Officer not to contact the employee. The Incident Resolution Service Team has determined that the 58 employees whose medical records were viewed will be sent HIPAA notification letters.

DBCT Decision Date: 10/06/2015

DBCT: The Data Breach Core Team has concurred with the decision of the Incident Resolution Service Team.

Security Privacy Ticket Number: PSETS0000124336

DBCT Category: Mishandling

Organization: VISN 20
Seattle, WA

Date Opened: 9/8/2015

Date Closed: 9/15/2015

Date of Initial DBCT Review: 9/15/2015

No. of Credit Monitoring: 59

No. of Loss Notifications: 4

Incident Summary

On 09/08/15, the Privacy Officer (PO) was advised that on 09/01/15, an employee in the VAPSHCS Release of Information (ROI) accidently released a compact disk containing the complete medical records for 70 Veterans to a single Veteran. The Veteran noticed the error after taking the CD home. He contacted the VAPSHCS and returned the compact disk on 09/08/15 at 9:00 AM.

Incident Update

09/10/15:
The final count of affected Veterans is 63. The Incident Resolution Service Team has determined that 59 Veterans will be sent a letter offering credit protection services and a notification letter will be sent to the Next of Kin for four Veterans.

Resolution

Both employees involved re-accomplished their annual privacy and HIPAA training. The employees are being counseled as appropriate by management.

DBCT Decision Date: 09/15/2015

DBCT: The Data Breach Core Team has concurred with the decision of the Incident Resolution Service Team.

Security Privacy Ticket Number: PSETS0000124505

DBCT Category: Mishandling

Organization: VISN 05
Baltimore, MD

Date Opened: 9/11/2015

Date Closed: 9/25/2015

Date of Initial DBCT Review: 9/22/2015

No. of Credit Monitoring: 76

No. of Loss Notifications:

Incident Summary

On 08/17/15 a Medical Support Assistant (MSA) was given a list of patients by the Acting Chief of Optometry to reschedule appointments. On 08/21/15, the MSA reported to his acting supervisor that the paperwork was missing. The MSA was asked to check with other staff members for its location and on 08/31/15 the MSA informed her supervisor that the paperwork is still missing. On 09/02/15, another search was conducted with no results. On 09/03/15 the Privacy Officer (PO) suggested that the Shred-it bins in the local area be checked, as it may have inadvertently been placed there. As suggested, the service requested that the bins be unlocked and a search was conducted with negative results. The list contained the first name, last name and full SSN.

Incident Update

09/14/15:
The Incident Resolution Service Team has determined that 43 Veterans will be sent letters offering credit protection services.

09/17/15:
The Privacy Officer has requested an additional 33 Promo Codes for credit protection services for a total of 76. This ticket will now go before the DBCT on 9/22/15.

Resolution

Staff members were re-educated on the proper handling of patient information to help prevent this type of incident from happening again.

DBCT Decision Date: 09/22/2015

DBCT: This incident was briefed to the Data Breach Core Team due to the number of Veterans affected. The Data Breach Core Team concurred with the decision of the Incident Resolution Service Team.

Security Privacy Ticket Number: PSETS0000124551

DBCT Category: CMOP Mismailed

Organization: VHA CMOP
Chelmsford, MA

Date Opened: 9/14/2015

Date Closed: 10/6/2015

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

Patient A received a Medline Industries medical supply intended for Patient B. Patient B's name and type of medical supply was compromised. Patient A reported the incident to the Connecticut Healthcare System West Haven Campus VA Medical Center and a replacement has been requested for Patient B. Chelmsford Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a Medline packing error. The packing error has been reported to Medline for investigation and corrective action.

Incident Update

09/14/15:
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 9/14/15, the packing error was reported to Medline for investigation and corrective action.

DBCT Decision Date:

DBCT: No DBCT decision is required. This is informational for Mis-Mailed CMOP incidents and is the representative ticket. There were only five Mis-Mailed CMOP incidents out of 7,151,070, total packages (10,269,491 total prescriptions) mailed out for this reporting period. In this incident, the affected individual will receive a HIPAA notification letter.

Security Privacy Ticket Number: PSETS0000124955

DBCT Category: Mishandling

Organization: VISN 21
Honolulu, HI

Date Opened: 9/22/2015

Date Closed: 9/29/2015

Date of Initial DBCT Review: 9/29/2015

No. of Credit Monitoring:

No. of Loss Notifications: 408

Incident Summary

On 09/17/15 Primary Care staff mailed 408 letters to Veterans notifying them of a newly assigned Primary Care Provider. The mail merge program dropped two lines during formatting, causing the names and corresponding addresses to be skewed. The letter identified the Veteran and the name of their Primary Care Provider.

Incident Update

09/23/15:
On 09/22/15 Primary Care was contacted by two Veterans claiming they had received another Veteran's mail. Two other Veterans delivered hard copies of letters to the Privacy Officer. Primary Care immediately notified the Privacy Officer, who reported the incident. The Incident Resolution Service Team has determined that 408 Veterans will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

408 Notification letters sent to Veterans. Please close this ticket. Education provide to staff on slowing down and QA sample of every mass mailing.

DBCT Decision Date: 9/29/2015

DBCT: The Data Breach Core Team has concurred with the decision of the Incident Resolution Service Team.

Security Privacy Ticket Number: PSETS0000125003

DBCT Category: Mishandling

Organization: VISN 08
Bay Pines, FL

Date Opened: 9/23/2015

Date Closed:

Date of Initial DBCT Review: 9/29/2015

No. of Credit Monitoring: 53

No. of Loss Notifications:

Incident Summary

The Business Office Service (BOS) reported that while processing the authorizations for February, they were unable to locate 53 Veteran authorizations. BOS has exhausted all search efforts to locate the authorizations.

Incident Update

09/23/15:
The Incident Resolution Service Team has determined that 53 Veterans will be sent letters offering credit protection services.

DBCT Decision Date: 09/29/2015

DBCT: The Data Breach Core Team concurred with the decision of the Incident Resolution Service Team to offor credit protection services due to the loss of Personally Identifiable Information.

Security Privacy Ticket Number: PSETS0000125277

DBCT Category:

Organization: VISN 08
Miami, FL

Date Opened: 9/29/2015

Date Closed:

Date of Initial DBCT Review: 10/6/2015

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

An employee who was angry with her supervisor began using her personal cell phone to take pictures of patient records (orders) that were displayed on a computer.

Incident Update

09/29/15:
The ISO has been asked the following questions:
Have the pictures been deleted off of the employee's camera?
Had she sent the pictures anywhere else (social media, cloud storage, another phone)?

10/05/15:
This incident is still under investigation. It is not known how many pictures she may have taken. The employee has been off work since the event occurred and is scheduled to be back in the office on Wednesday 10/07/15.

DBCT Decision Date:

DBCT: This incident is still under review by the Data Breach Core Team pending additional information to be gathered.