Information Security
Monthly Activity Report*

INFOCON LEVEL
CRITICAL
SEVERE
ELEVATED
GUARDED
NORMAL

April 2016

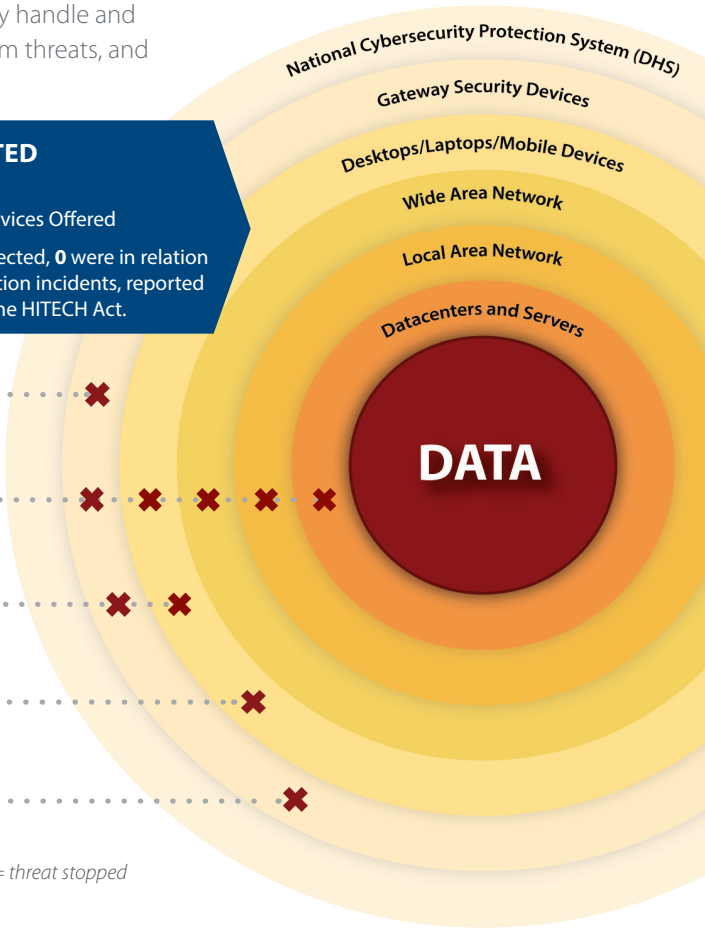
VA uses a defense-in-depth approach to information security to protect the data we hold on Veterans. While the defense-in-depth approach protects from inbound threats and contains other data exposing incidents, VA relies on employees to protect Veteran information they handle and transmit. This graphic 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)
77,690,668

Malware (Blocked/Contained)
459,792,918

Suspicious/Malicious Emails (Blocked)
105,391,356

Infected Medical Devices (Contained)
2

Outgoing Unencrypted Emails
67 Associated Privacy/Security Events
28,549 Total Emails Blocked

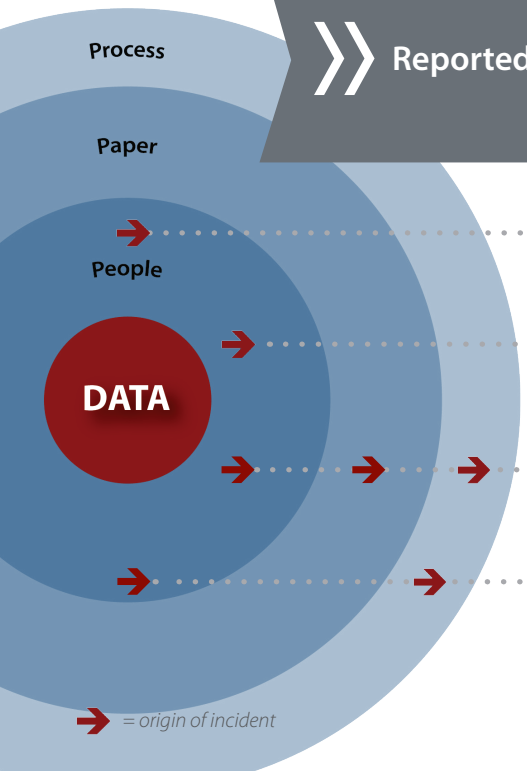
✖ = threat stopped

Reported Events

2,556 VETERANS AFFECTED

1,690 Notifications
866 Credit Protection Services Offered

Of the total # of Veterans affected, **2,105** were in relation to protected health information incidents, reported to HHS in accordance with the HITECH Act.



Lost and Stolen Device Incidents
39

Lost PIV Cards
128

Mishandled Incidents
87

Mis-mailed Incidents
146 Paper Mis-mailings
6 Pharmacy-item Mis-mailings
out of **6,532,811** 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
Data Breach Response Service

Monthly Report to Congress of Data Incidents

April 1-30, 2016

Security Privacy Ticket Number: PSETS0000133756

DBCT Category: Mismailed

Organization: VBA
Chicago, IL

Date Opened: 4/1/2016

Date Closed: 4/1/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

Veteran A received a notification letter belonging to Veteran B. The letter was contained in the same envelope as his own.

Incident Update

04/01/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that Veteran B will be sent a notification letter.

Resolution

Mailroom employees and their supervisor will be briefed on increasing incidents involving envelopes containing more than one Veteran's correspondence.

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 146 Mis-Mailed incidents this reporting period. Because of repetition, the other 145 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: PSETS0000133796

DBCT Category: Mishandling

Organization: VISN 01
West Haven, CT

Date Opened: 4/1/2016

Date Closed: 4/7/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

Appointment reminder messages were left on the wrong person's answering machine.

Incident Update

04/04/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that the Veteran will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

Employees were counseled on the importance of verifying the correct phone number.

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 87 Mis-Handling incidents this reporting period. Because of repetition, the other 86 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:	PSETS0000133798
DBCT Category:	Mishandling
Organization:	VBA Ft Harrison, MT
Date Opened:	4/1/2016
Date Closed:	4/14/2016
Date of Initial DBCT Review:	4/5/2016
No. of Credit Monitoring:	162
No. of Loss Notifications:	

Incident Summary

A Vocational Rehabilitation and Employment (VR&E) representative sent an unencrypted email to a Veteran with an attachment that contained other Veterans names and SSNs. The email was sent to a yahoo.com account.

Incident Update

04/04/16:
The investigation revealed that the employee was a VR&E Counselor who was sending routine correspondence to a Veteran. While including in the email a necessary attachment, an incorrect attachment was inadvertently included which contained the full name and full SSN for 162 Veterans. The mistake was immediately noticed and contact was made with the Veteran who is being very cooperative and has agreed to delete the attachment.

04/05/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Core Team has determined that 162 Veterans will be sent letters offering credit protection services.

Resolution

The Veteran was contacted and the email was deleted from her inbox and her deleted items in her yahoo account. She did not copy, download, or save this email in any way. The Veteran has confirmed deletion of the email and that this information was not improperly used or further disclosed.

DBCT Decision Date: 04/05/2016

DBCT

The DBCT has determined that 162 affected individuals will be sent a letter offering Credit Protection Services.

Security Privacy Ticket Number: PSETS0000133842

DBCT Category: Mishandling

Organization: VISN 08
Bay Pines, FL

Date Opened: 4/4/2016

Date Closed: 4/15/2016

Date of Initial DBCT Review: 4/12/2016

No. of Credit Monitoring:

No. of Loss Notifications: 103

Incident Summary

A VA lawn maintenance worker found a Housing and Urban Development Veterans Affairs Supportive Housing (HUD VASH) Veteran contact list outside. The documents were secured and given to the HUD VASH Supervisor. The Privacy Officer (PO) is following up with the Supervisor to determine how long the documents were unsecured and unattended outside.

Incident Update

The Facility Incident Resolution Team met to discuss this incident. It is reported that 103 Veterans are affected. The employee stated she took the documents out of the building at 2:00 PM and noticed they were gone at 3:30 PM. The Environmental Management Service (EMS) employee reported finding the documents sometime after 1:00 PM. The Social Work supervisor reported the documents were given to her by the EMS employee sometime after 3:30 PM. It remains unknown how long the documents were on the lawn. VA Police conducted an exterior search of all the parking lots around the building and the wood line on the southern edge with negative results of further documents in the area.

04/06/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 103 Veterans will be sent a general notification letter.

Resolution

A privacy violation memo was issued. Service Management will propose appropriate disciplinary action for the employee involved in the privacy violation and staff will be educated about unauthorized logbooks.

DBCT Decision Date: 04/12/2016

DBCT The Data Breach Core Team reviewed this event and concurred that 103 Veterans will be sent a HIPAA notification letter.

Security Privacy Ticket Number: PSETS0000133963

DBCT Category: CMOP Mismailed

Organization: VHA CMOP
Charleston, SC

Date Opened: 4/6/2016

Date Closed: 4/21/2016

Date of Initial DBCT Review: N/A

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 Orlando VA Medical Center and a replacement has been requested for Patient B. Charleston Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error. The CMOP employee(s) will be counseled and retrained in proper packing procedures.

Incident Update

04/06/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that Veteran B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

On 4/6/2016, 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 six Mis-Mailed CMOP incidents out of 6,532,811 total packages (9,620,989) total prescriptions) mailed out for this reporting period. Because of repetition, the other 6,532,805 are not included in this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number: PSETS0000134596

DBCT Category: Mishandling

Organization: VISN 12
Hines, IL

Date Opened: 4/18/2016

Date Closed:

Date of Initial DBCT Review: 4/19/2016

No. of Credit Monitoring:

No. of Loss Notifications: 235

Incident Summary

A Prosthetics Program Support Assistant (PSA) reported that a package full of approximately 235 patients' home-oxygen information was mailed from Madison VA on March 25, 2016, via USPS. Such packages are first run through the VA North Central Consolidated Patient Account Center (NCCPAC) for consolidated shipping. On April 5, 2016, the PSA attempted to track the package which had not yet been received. On April 12, 2016 a broadcast message was sent to all MIW VA employees to attempt to locate the package, had it been delivered to another department. No response was received. As of April 18, 2016, the package still had not arrived, and several points of contact have replied that they are not able to determine where the package is.

Incident Update

04/26/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 235 Veterans will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

DBCT Decision Date: 04/19/2016

DBCT

The Data Breach Core Team reviewed this event and concurred that 235 Veterans will be sent a HIPAA notification letter.

Security Privacy Ticket Number: PSETS0000135145

DBCT Category: Mishandling

Organization: VISN 22
Las Vegas, NV

Date Opened: 4/27/2016

Date Closed:

Date of Initial DBCT Review: 5/3/2016

No. of Credit Monitoring: 28

No. of Loss Notifications: 84

Incident Summary

An unknown employee removed documents pertaining to Claims not approved, TORTS, and Billing. Set on the roof of car and drove off, items fell onto a public highway and were collected by unknown citizen and turned in.

Incident Update

04/29/16:
The Privacy Officer is not able to verify how long the information was missing. The documents involve 28 Veterans with full name, address, Date of Birth and gender. Other documents involve 84 Veterans with full name and claim numbers. It looks as if someone took them home, then as they were driving to work they came off the roof of the car. They were in a regular envelope and not the required red locked bags and located nowhere near a VA facility. After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 28 Veterans will be sent a letter offering credit protection services. A notification letter will be sent to 84 Veterans.

DBCT Decision Date: 05/03/2016

DBCT

The Data Breach Core Team concurred that Credit Protection Services will be offered to 28 Veterans and 84 Veterans will be sent a HIPAA notification letter.

Security Privacy Ticket Number: PSETS0000135154

DBCT Category: IT Equipment Inventory

Organization: VISN 06
Hampton, VA

Date Opened: 4/27/2016

Date Closed:

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

During an equipment inventory 14 computers with encrypted hard drives could not be accounted for.

Incident Update

04/28/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, § C (Risk Assessment), Paragraph 1 (d), the Data Breach Response Service has determined that no breach has occurred. The missing Hard Drives were all encrypted. Therefore this incident has a low probability of a risk of compromise due to the risk having been properly mitigated through established controls.

DBCT Decision Date:

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 a total of three IT Equipment Inventory Incidents this reporting period. Because of repetition, the other two are not included in this report.