DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Data Breach Response Service

Monthly Report to Congress of Data Incidents

May 1 - May 31, 2016

Security Privacy Event Number: PSETS0000135400

DBCT Category: IT Equipment Inventory

Organization: VBA
Manchester, NH

Date Opened: 5/3/2016

Date Closed: 5/9/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

During an inventory, it was noticed that IT equipment was missing from the IT office and computer room. The equipment consisted of one laptop, two monitors, two Bluetooth keyboards and four computer backpacks. The laptop had not been imaged for VA use and did not contain any PHI/PII and had not been issued, it was new in the box.

Incident Update

05/03/16:
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 laptop had not been in service (new in the box). Therefore this incident has a low probability of a risk of compromise due to the risk having been properly mitigated through established controls.

Resolution

The facility liaison has reported this matter to GSA and other appropriate contacts.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for IT Equipment Inventory incidents and is the representative event. There were a total of two IT Equipment Inventory Incidents this reporting period. Because of repetition, the other incident is not included in this report, but is included in the "IT Equipment Inventory Incidents" count at the end of this report.

Security Privacy Event Number: PSETS0000135867

DBCT Category: Mismailed

Organization: VISN 15
St Louis, MO

Date Opened: 5/12/2016

Date Closed:

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 4

Incident Summary

Veteran A contacted the facility patient advocate regarding a pre-appointment letter that was received. When opened, inside the envelope, Veteran A found pre-appointment letters for four other Veterans. The Veteran was asked to return the letters to the VA.

Incident Update

05/12/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that four Veterans will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for Mis-Mailed incidents and is the representative event. There were a total of 125 Mis-Mailed incidents this reporting period. Because of repetition, the other 124 are not included in this report, but are included in the "Mis-Mailed Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Security Privacy Event Number: PSETS0000135881

DBCT Category: CMOP Mismailed

Organization: VHA CMOP
Murfreesboro, TN

Date Opened: 5/12/2016

Date Closed: 5/17/2016

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 medical center and a replacement has been requested for Patient B. Murfreesboro Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error. The CMOP employee was counseled and retrained in proper packing procedures.

Incident Update

05/12/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that Patient B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

On 5/12/2016, 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 event. There were a total of 14 Mis-Mailed CMOP incidents out of 6,613,065 total packages (9,775,782 total prescriptions) mailed out for this reporting period. Because of repetition, the other 13 are not included in this report, but are included in the "Mis-Mailed CMOP Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Event Number: PSETS0000136652

DBCT Category: Mishandling

Organization: VISN 06
Richmond, VA

Date Opened: 5/27/2016

Date Closed: 6/7/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring: 1

No. of Loss Notifications:

Incident Summary

Veteran A was discharged from their ward and went to the Pharmacy to review discharge medications with the Pharmacist. When the Pharmacist reviewed the Veteran's paperwork, the Pharmacist noticed that Veteran B's discharge summary and progress notes were attached to Veteran A's paperwork. The Pharmacist removed and recovered Veteran B's paperwork prior to Veteran A leaving the Pharmacy.

Incident Update

05/27/16:
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 letter offering credit protection services.

Resolution

The information was retrieved from the Veteran at the pharmacy; all staff has been provided with training on proper procedures.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for Mis-Handled incidents and is the representative event. There were a total of 106 Mis-Handled incidents this reporting period. Because of repetition, the other 105 are not included in this report, but are included in the "Mis-Handled Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

This page is blank.

DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Data Breach Response Service

Monthly Report to Congress of Data Incidents

June 1 - 30, 2016

Security Privacy Ticket Number: PSETS0000136870

DBCT Category: CMOP Mismailed

Organization: VHA CMOP
Leavenworth, KS

Date Opened: 6/2/2016

Date Closed: 6/20/2016

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 Iowa City VA Medical Center and a replacement has been requested for Patient B. The Leavenworth Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error.

Incident Update

06/02/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that Patient B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

06/24/16:
This HITECH event was reported to HHS/OCR this date. The Breach Tracking Number is HCQGBL53Y7.

Resolution

On 6/2/2016, 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 event. There were a total of 6 Mis-Mailed CMOP incidents out of 6,899,788 total packages (10,277,722 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 notification letters.

Security Privacy Ticket Number: PSETS0000136951

DBCT Category: IT Equipment Inventory

Organization: VISN 23
Iowa City, IA

Date Opened: 6/3/2016

Date Closed: 6/3/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

During a routine VA Logistics equipment inventory it was found that three devices capable of storing or transmitting VA Data could not be located.

Incident Update

06/03/16:
The three devices missing are: one DS3-IPS Chassis (a switch), one handheld radio frequency identification (RFID) Reader, and one Yorktel device. Immediately after the event was entered in PSETS the Yorktel device was found. Of the three devices, the Yorktel was the only item capable of storing sensitive data. No data breach has occurred.

Resolution

On 06/03/2016 the only device listed on the report of survey with the potential to store sensitive data was located in the VA facility's secure storage. No data has been lost.

DBCT Decision Date: N/A

DBCT

No DBCT decision is required. This is informational for IT Equipment Inventory incidents and is the representative event. There were a total of five IT Equipment Inventory Incidents this reporting period. Because of repetition, the other four incidents are not included in this report.

Security Privacy Ticket Number: PSETS0000137011

DBCT Category: Mismailed

Organization: VBA
Roanoke, VA

Date Opened: 6/6/2016

Date Closed: 6/7/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring: 1

No. of Loss Notifications:

Incident Summary

Veteran A received Veteran B's notification letter in error in the mail. The letter included Veteran B's name, address, and full SSN.

Incident Update

06/06/16:
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 letter offering credit protection services.

Resolution

The employee involved in this incident received training on 06/06/16 regarding proper handling of Veteran personally identifiable information (PII).

DBCT Decision Date: N/A

DBCT

No DBCT decision is required. This is informational for Mis-Mailed incidents and is the representative event. There were a total of 186 Mis-Mailed incidents this reporting period. Because of repetition, the other 185 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: PSETS0000137082

DBCT Category: Mishandling

Organization: VISN 10
Chillicothe, OH

Date Opened: 6/7/2016

Date Closed: 6/21/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring: 1

No. of Loss Notifications:

Incident Summary

Veteran A called the Radiology Department and stated that when he looked at a CD that he was provided earlier by VA staff, he saw that it contained radiology images of Veteran B.

Incident Update

06/07/16:
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 letter offering credit protection services.

Resolution

A malfunctioning equipment issue has been addressed by Radiology staff.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for Mis-Handled incidents and is the representative event. There were a total of 117 Mis-Handled incidents this reporting period. Because of repetition, the other 116 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:	PSETS0000138687
DBCT Category:	Missing/Stolen Equipment (Other)
Organization:	VISN 07 Charleston, SC
Date Opened:	6/16/2016
Date Closed:	
Date of Initial DBCT Review:	6/21/2016
No. of Credit Monitoring:	
No. of Loss Notifications:	992

Incident Summary

A contractor for the Ralph H. Johnson (Charleston, SC) VAMC lost one USB drive that was used in the process of fit-testing respirators for employees. He had the USB drive on 06/10/16 while fit-testing employees at the Myrtle Beach Outpatient Clinic (OPC). A VA employee noticed the USB drive was missing on 06/13/16 when he was setting up the equipment back at the medical center. The VA employee notified the contractor and the nurse supervisor at the Myrtle Beach OPC. The nurse supervisor reported that she did not find it in the room used by the contractor. The contractor requested more time to find the USB drive, which may have been left in the rental car that was used to drive to Myrtle Beach. The rental car company was contacted, and they responded that it had not been found, but the car was being used again and they would search it again when returned.

Incident Update

06/20/16:
The facility is waiting to hear back from the rental agency.

06/21/16:
The rental car agency has not found the thumb drive yet. The contractor does have a national Business Associate Agreement. The PO is still trying to confirm if the device was FIPS compliant and encrypted.

6/23/16:
After speaking to the IT technician for the contractor, he did confirm that the thumb drive was not encrypted, because an encrypted thumb drive could not be used in the PortaCount device. The data is an XML file. The data on the thumb drive is basic in nature. A respirator fit-test size is required to ensure a secure fit and can change based on having a beard, losing weight, dental work, and using a different manufacture/vendor. Based on the above information and due to the fact that XML format can be decoded, there is potential for a data breach. A total of 992 employee names and partial SSNs were stored on the USB drive.

06/28/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 992 employees will be sent notification letters.

DBCT Decision Date: 06/28/2016

DBCT

DBCT concurs with the Data Breach Response Service that this is a breach and that a general notification letter should be sent to each employee involved.

Security Privacy Ticket Number: PSETS0000138898

DBCT Category: Mishandling

Organization: VISN 08
Bay Pines, FL

Date Opened: 6/21/2016

Date Closed:

Date of Initial DBCT Review: 6/21/2016

No. of Credit Monitoring: 235

No. of Loss Notifications: 22

Incident Summary

The Business Office Service reported that 386 requests for medical records cannot be found.

Incident Update

06/21/16:
It is unknown exactly what personally identifiable information was on the forms, but if an individual uses the VA request form, it would include the patient's name and SSN. If other (non-VA) forms were used, it is not clear exactly what information would be on the form, but the SSN would be probable.

07/05/16:
They are still searching but the number of lost items now stands at 394 and the search will be concluded by 07/08/16.

07/12/16:
After duplicates have been removed the totals are 235 living and 22 deceased Veterans whose information has been lost.

DBCT Decision Date: 07/12/2016

DBCT

07/12/16:
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 letters offering credit protection services and 22 next-of-kin notifications will be sent.

Security Privacy Ticket Number: PSETS0000139120

DBCT Category: Mishandling

Organization: VISN 01
West Haven, CT

Date Opened: 6/24/2016

Date Closed:

Date of Initial DBCT Review: 7/12/2016

No. of Credit Monitoring: 294

No. of Loss Notifications:

Incident Summary

The Privacy Officer (PO) was notified by an anesthesiologist that a logbook containing approximately 50 patients' names, full SSNs and dates of birth was noted to be missing The book has been missing for approximately two weeks before it was reported. They are looking in the area which is locked to find the misplaced book.

Incident Update

07/08/16:
After further investigation, it has been determined the logbook included information on 294 Veterans. The PO reports that there were names, dates of birth and full SSNs for many of the 294 patients. They have a list of the patients but do not know the exact information that was missing on each one. On some they used the patient label which contained full SSN and date of birth, and on others they just used the name and last four numbers of the SSN. This was not an approved logbook.

DBCT Decision Date: 07/12/2016

DBCT

07/12/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that all 294 Veterans will be sent letters offering credit protection services.

Page left blank.

DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Data Breach Response Service

Monthly Report to Congress of Data Incidents

July 1 - 31, 2016

Security Privacy Ticket Number: PSETS0000139539

DBCT Category: Mishandling

Organization: VISN 06
Richmond, VA

Date Opened: 7/1/2016

Date Closed: 7/15/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring: 1

No. of Loss Notifications:

Incident Summary

Veteran A was inadvertently given Veteran B's lab results. Veteran A returned Veteran B's lab results the following day.

Incident Update

07/01/16:
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 letter offering credit protection services.

Resolution

Retrieval, training and awareness was provided to staff. The credit protection services letter was uploaded on 7/15/2016 and mailed to the Veteran.

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 86 Mis-Handling incidents this reporting period. Because of repetition, the other 85 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: PSETS0000139665

DBCT Category: Mismailed

Organization: VBA
Oakland, CA

Date Opened: 7/6/2016

Date Closed: 7/8/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring: 1

No. of Loss Notifications:

Incident Summary

Veteran A received correspondence from the VA that included a letter addressed to Veteran B.

Incident Update

07/06/16:
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 letter offering credit protection services.

Resolution

Employees were reminded of the importance of having only one Veteran's correspondence in each outgoing envelope.

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 128 Mis-Mailed incidents this reporting period. Because of repetition, the other 127 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:	PSETS0000139680
DBCT Category:	Mishandling
Organization:	VBA Fargo, ND
Date Opened:	7/6/2016
Date Closed:	8/9/2016
Date of Initial DBCT Review:	7/26/2016
No. of Credit Monitoring:	62
No. of Loss Notifications:	

Incident Summary

The ex-wife of a former telework employee discovered 62 pieces of returned mail while cleaning out a file cabinet. She returned the documents to the Police Service at the local VAMC.

Incident Update

07/06/16:
The employee is still a VA employee but has transferred to another Regional Office. This is being investigated by the facility.

07/25/16:
The facility did not contact the ex-spouse and the Privacy Office (PO) has not spoken with the employee to investigate further. After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 62 Veterans will be sent letters offering credit protection services.

Resolution

The employee does not work at this station; however, the information was relayed to the Director and management staff at his new Regional Office (RO). Letters offering credit protection have been sent.

DBCT Decision Date: 07/26/2016

DBCT

DBCT concurred that this was a data breach. This is informational due to the number of Veterans affected.

Security Privacy Ticket Number: PSETS0000139801

DBCT Category: Unencrypted Laptop Missing

Organization: VISN 01
Boston, MA

Date Opened: 7/8/2016

Date Closed: 7/11/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

The following laptops were discovered missing from the warehouse (WX campus, BLDG 22, room 7):

EE#	S/N
149091	7HL4LX1
149087	F26CSY1
149089	GG5CSY1
149090	DFGCSY1
149092	CHK4LX1

Last visual accountability was on May 4, 2016 by the employee. The Information Security Officer (ISO) and the police have checked the location and will continue the investigation. The laptops were brand-new with no VA image and contained no VA information.

Incident Update

07/08/16:
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 laptops were not encrypted, but had never been used, thus contained no VA sensitive or patient data.

Resolution

All employees have been educated and key control, inventory processes have been reviewed.
No Personally Identifiable Information (PII) or Protected Health Information (PHI) was on these laptops.

Security Privacy Ticket Number: PSETS0000140226

DBCT Category: Mishandling

Organization: VISN 21
San Francisco, CA

Date Opened: 7/18/2016

Date Closed:

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 102

Incident Summary

On Saturday July 16, 2016 around noon, a research assistant discovered her car, which was parked in the VA parking lot, was broken into. She indicated that a bag, containing a research binder, was stolen. The binder contained multiple sheets of paper that included VA patient's identifiers such as contact phone numbers, first name, last name, and last 4 digits of social security number. There were approximately 102 patients listed in the stolen documents. The researcher reported the incident to VA police immediately.

Incident Update

07/19/16:
Research staff can identify all patients included in the research binder. The participant log contained a recruitment flyer and the participant's first and last name, appointment time and date, phone number, and last four numbers of SSN. After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 102 Veterans will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

DBCT Decision Date:

DBCT
No DBCT decision needed. This is informational due to the number of Veterans affected.

Security Privacy Ticket Number: PSETS0000140522

DBCT Category: Unencrypted Desktop Stolen

Organization: VISN 08
Miami, FL

Date Opened: 7/22/2016

Date Closed:

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

A thief was arrested by VA police in the first floor on July 21, 2016 at 6:30 PM. Afterward the suspect stated to the police that he had two computers at home . VA police went to the suspect home and recovered a third stolen computer that the VA was not aware was stolen.

Incident Update

07/27/16:
Three devices were stolen, two of which were encrypted PC's. One was a laptop that was connected to an eye scanner that was not encrypted (as a bio-medical device). The suspect was arrested and the equipment returned the day it was stolen. The ISO has confirmed that the device that was not encrypted was not logged onto during the hours that it was in the possession of the suspect. 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, as the other two devices were encrypted. Therefore, this incident has a low probability of a risk of compromise due to the risk having been properly mitigated through established controls.

Security Privacy Ticket Number: PSETS0000140847

DBCT Category: IT Equipment Inventory

Organization: MANAGEMENT - 004B
Washington, DC

Date Opened: 7/28/2016

Date Closed:

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

The BlackBerry on the attached Report of Survey (ROS) was not located at the conclusion of the FY16 July Inventory.

Incident Update

07/28/16:
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. All of the devices were encrypted per policy. 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: 8/2/2016

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 8 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 7 are not included in this report.

Security Privacy Ticket Number:	PSETS0000140927
DBCT Category:	CMOP Mismailed
Organization:	VHA CMOP Hines, IL
Date Opened:	7/29/2016
Date Closed:	8/11/2016
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 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

07/29/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that Patient B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

On 7/29/2016, 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 8 Mis-Mailed CMOP incidents out of 6,311,830 total packages (9,383,409 total prescriptions) mailed out for this reporting period. Because of repetition, the other 7 are not included in this report. In all incidents, Veterans will receive a notification letter.

Page left blank.

DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Data Breach Response Service

Monthly Report to Congress of Data Incidents

August 1 - 31, 2016

Security Privacy Ticket Number:	PSETS0000140991
DBCT Category:	Mismailed
Organization:	VISN 01 Providence, RI
Date Opened:	8/1/2016
Date Closed:	8/9/2016
Date of Initial DBCT Review:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	1

Incident Summary

Veteran A called to say he had received a cancer results letter for Veteran B. Veteran A states the letter was addressed to his address but contained a letter for Veteran B.

Incident Update

08/01/16:
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 HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

The Privacy Officer discussed this with the Primary Care Team asking them to give more attention when stuffing envelopes, the notification letter was sent to the Veteran.

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 149 Mis-Mailed incidents this reporting period. Because of repetition, the other 148 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:	PSETS0000140994
DBCT Category:	CMOP Mismailed
Organization:	VHA CMOP Dallas, TX
Date Opened:	8/1/2016
Date Closed:	8/3/2016
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 Medical Center and a replacement has been requested for Patient B. 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

08/01/16:
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 HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

On 8/1/2016, 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 9 Mis-Mailed CMOP incidents out of 6,954,630 total packages (10,319,106 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: PSETS0000141027

DBCT Category: Mishandling

Organization: VISN 01
Boston, MA

Date Opened: 8/2/2016

Date Closed: 8/25/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring: 1

No. of Loss Notifications:

Incident Summary

A pharmacy outpatient order sheet was found in the parking lot yesterday afternoon by an EMS staff member who turned it in to VA Police.

Incident Update

08/09/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that Veteran A will be sent a letter offering credit protection services.

Resolution

The Document was retrieved and the Veteran was sent a letter offering credit protection services.

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 99 Mis-Handling incidents this reporting period. Because of repetition, the other 98 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: PSETS0000141358

DBCT Category: IT Equipment Inventory

Organization: VACO OI&T
Washington, DC

Date Opened: 8/9/2016

Date Closed:

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

During a June 2016 inventory, a monitor was not located. The Report of Survey (ROS) is attached.

Incident Update

08/09/16:
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 device is not data capable.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for IT Equipment Inventory incidents and is the representative ticket. This was the only IT Equipment Inventory Incident this reporting period.

Page left blank.

DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Data Breach Response Service

Monthly Report to Congress of Data Incidents

September 1 – 30, 2016

Security Privacy Ticket Number: PSETS0000142574

DBCT Category: Mismailed

Organization: VBA
St Paul, MN

Date Opened: 9/1/2016

Date Closed: 9/9/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

Widow A received a letter that contained another letter belonging to widow B. The name and SSN belonging to the deceased Veteran of widow B was disclosed.

Incident Update

09/01/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that Veteran B's Next of Kin will be sent a notification letter.

Resolution

The supervisor provided PII awareness training to the responsible team members on 08/23/16.

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 167 Mis-Mailed incidents this reporting period. Because of repetition, the other 166 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: PSETS0000142578

DBCT Category: Mishandling

Organization: VISN 11
Indianapolis, IN

Date Opened: 9/1/2016

Date Closed:

Date of Initial DBCT Review: N/A

No. of Credit Monitoring: 1

No. of Loss Notifications:

Incident Summary

An employee gave Veteran A's medical consult to Veteran B.

Incident Update

09/01/16:
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 letter offering credit protection services.

Resolution

Employee received verbal counseling

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 108 Mis-Handling incidents this reporting period. Because of repetition, the other 107 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: PSETS0000142595

DBCT Category: IT Equipment Inventory

Organization: VACO OI&T
Washington, DC

Date Opened: 9/1/2016

Date Closed: 9/1/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

On 08/31/16, during physical inventory, two thin clients could not be accounted for. Thin clients do not store data and do not contain hard drives.

Incident Update

09/01/16:
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 devices were not capable of storing VA data. Therefore this incident has a low probability of a risk of compromise due to the risk having been properly mitigated through established controls.

Resolution

No violation was found since the devices are not capable of storing VA data.

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

Security Privacy Ticket Number:	PSETS0000142928
DBCT Category:	Mishandling
Organization:	VISN 06 Beckley, WV
Date Opened:	9/8/2016
Date Closed:	9/16/2016
Date of Initial DBCT Review:	9/13/2016
No. of Credit Monitoring:	150
No. of Loss Notifications:	

Incident Summary

On 09/08/16 at approximately 9:25 a.m. employees stopped by to inform the Privacy Officer that a 3-ring white binder with a picture of a telephone on top of the binder is missing. In the notebook are completed Patient Satisfaction Discharge Call Back forms on discharged patients for the months of July and August, 2016 (estimate of 70-80 patients). On each completed form there will be a label with the patient's full name, full SSN, and date birth. On 09/06/16, in the a.m. the employees went to look for this notebook and were told by a staff member that they have not been able to locate it. The notebook was last used and seen by an ICU RN who advised that when she was through with the notebook she placed it beside the telemetry monitor. The PO was informed that they have looked everywhere for the notebook and so far they cannot find it.
The creation of this notebook was unapproved for usage and is considered an unapproved logbook.

Incident Update

09/13/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 150 Veterans will be sent letters offering credit protection services.

Resolution

The information from the Patient Satisfaction Discharge Call Back forms has been implemented electronically. The notebook will no longer be used. That was a log book and is against the rules to use for this very reason. The notebook is now missing with 150 Veterans PII placing them at risk for identity theft, etc. On 9/19/16 the Privacy Officer (PO) will send an e-mail to all staff stressing that log books are prohibited unless approved by the Director and give an explanation as to what is considered a logbook. In the near future, the PO will schedule and attend some of the larger staff meetings to talk about the prohibition of logbooks unless approved by the Director and give an explanation as to what is considered a logbook. Since 9/10/16, the PO has been trying to call the affected Veterans to let them know what happened and to expect a letter from the Director offering one year of free credit monitoring. The PO will complete calls on the evening of 09/15/16 and whoever was not contacted can call the PO with any questions. All nursing units are looking at all of their processes to ensure that whatever can be converted to electronic logs from paper records. The PO educated the staff and Assistant Chief as to what a logbook is considered since none of them felt the missing notebook would be considered a logbook. All letters were mailed to the affected Veterans on 9/15/16 by USPS certified mail.

DBCT Decision Date: 09/13/2016

DBCT

Due to the numbers affected, the DBCT reviewed this event for awareness and concurred that 150 Veterans will be sent a letter offering credit protection services.

Security Privacy Ticket Number: PSETS0000142965

DBCT Category: Mishandling

Organization: VISN 23
Minneapolis, MN

Date Opened: 9/8/2016

Date Closed:

Date of Initial DBCT Review: 9/20/2016

No. of Credit Monitoring: 351

No. of Loss Notifications:

Incident Summary

Copies of prosthetic device information from various vendors went missing during an office relocation. Not every copy includes the same information. All ask for patient name, date of birth, gender, and type of surgery. Not all ask for the social security number, but some do. The Privacy Officer has a listing of all patients that could be potentially impacted to include those who had social security numbers on the device identification. The preliminary count of potentially affected individuals is 520.

Incident Update

09/20/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Core Team has determined that 440 Veterans will be sent letters offering credit protection services.

09/29/16:
After a removal of duplicates and non-applicable names, the new number of affected individuals is 351.

DBCT Decision Date: 09/20/2016

DBCT

09/20/16:
The DBCT concurred that 351 affected Veterans will be sent a letter offering credit protection services.

Security Privacy Ticket Number: PSETS0000142973

DBCT Category: CMOP Mismailed

Organization: VHA CMOP
Tucson, AZ

Date Opened: 9/8/2016

Date Closed: 9/14/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

Patient A received one non-controlled medication with prescription information for patient B. This incident was identified at the Southwest VA CMOP. The CMOP contacted the patient to verify the accuracy of the prescription label. The patient reported their medication label contained another patient's name, prescription number, provider name, medication name and directions. The CMOP sent a prepaid envelope to collect the incorrectly printed medication and it is now in CMOP possession. The medication contents were correct despite the incorrect information listed on the prescription label. Patient A did not take any of the medication. The CMOP has contacted the VAMC to resubmit the prescription.

Incident Update

09/09/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that patient B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

On 09/08/2016, the printer malfunction was corrected.

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 11 Mis-Mailed CMOP incidents out of 6,663,171 total packages (9,896,883 total prescriptions) mailed out for this reporting period. Because of repetition, the other 10 are not included in this report. In all incidents, Veterans will receive a notification letter.

Page left blank

DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Data Breach Response Service

Monthly Report to Congress of Data Incidents

October 1-31, 2016

Security Privacy Ticket Number: PSETS0000144239

DBCT Category: IT Equipment Inventory

Organization: VISN 23
Omaha, NE

Date Opened: 10/4/2016

Date Closed: 10/26/2016

Date of Initial DBCT Review: 10/11/2016

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

Local Office of Information and Technology (OI&T) staff have completed the annual inventory and multiple items were noted as missing, including servers and PC's. Local OI&T staff have initiated a Report of Survey to document all of the missing items.

Incident Update

10/11/16:
A review of the inventory list indicates the data capable devices missing to be eight desktops and six servers. The ISO will be verifying with IT staff that the missing devices were or were not encrypted.

10/25/16:
The PC's were encrypted and the servers have all been located.

10/26/16:
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 desktops were encrypted. Therefore this incident has a low probability of a risk of compromise due to the risk having been properly mitigated through established controls. Additionally, the servers have been located.

Resolution

The missing servers have been accounted for. The investigation results lead the facility to believe this to be a case of inventory control error (not theft), and that all other assets will be accounted for.

DBCT Decision Date: 10/25/2016

DBCT

Though the DBCT did review this, no DBCT decision is required. This is informational for IT Equipment Inventory incidents and is the representative ticket. There were four IT Equipment Inventory Incidents this reporting period. Because of repitition, the other three incidents are not included in this report.

Security Privacy Ticket Number: PSETS0000144912

DBCT Category: Mishandling

Organization: VISN 22
Los Angeles, CA

Date Opened: 10/19/2016

Date Closed:

Date of Initial DBCT Review: N/A

No. of Credit Monitoring: 1

No. of Loss Notifications:

Incident Summary

A nurse practitioner (NP) accidently gave patient B's lab results containing his full name, full SSN, and date of birth to patient A. Both patients were notified of the mistake by the NP prior to reporting it to the Privacy Officer. Patient B has not returned the lab results and has stated to the NP that he will shred them and has not looked at them.

Incident Update

10/19/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that patient B will be sent a letter offering credit protection services.

Resolution

The nurse practitioner self-reported the incident and is aware of her mistake.

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 82 Mis-Handling incidents this reporting period. Because of repetition, the other 81 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: PSETS0000145008

DBCT Category: CMOP Mismailed

Organization: VHA CMOP
Leavenworth, KS

Date Opened: 10/21/2016

Date Closed: 11/1/2016

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 Omaha VA Medical Center and a replacement has been requested for Patient B. Leavenworth 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

10/21/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that Patient B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

On 10/21/16, 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 three Mis-Mailed CMOP incidents out of 6,552,321total packages (9,591,561 total prescriptions) mailed out for this reporting period. Because of repetition, the other two are not included in this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number: PSETS0000145183

DBCT Category: Mismailed

Organization: VISN 06
Salem, VA

Date Opened: 10/26/2016

Date Closed: 10/27/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring: 1

No. of Loss Notifications:

Incident Summary

Veteran A received a mailing that had a consult sheet in the envelope for Veteran B. Using the address on the consult sheet, Veteran A mailed the sheet to Veteran B. Veteran B brought it to the Patient Advocate with the envelope it was mailed in.

Incident Update

10/26/16:
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 letter offering credit protection services.

Resolution

The paperwork has been retrieved and the CBOC staff were asked to look at each page of each mailing before sealing the envelope to prevent this from happening in the future.

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 144 Mis-Mailed incidents this reporting period. Because of repetition, the other 143 are not included in this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Page left blank

DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Data Breach Response Service

Monthly Report to Congress of Data Incidents

November 1 – 30, 2016

Security Privacy Event Number: PSETS0000145488

DBCT Category: Mishandling

Organization: VISN 04
Lebanon, PA

Date Opened: 11/1/2016

Date Closed: 11/23/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

Veteran A received Veteran B's medication paperwork. The paperwork was returned to the Lebanon VA.

Incident Update

11/01/16:
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 HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

This supervisor addressed this issue with the employee and will remind staff to separate paperwork more carefully. Veteran B has been sent a HIPAA Notification Letter.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for Mishandling incidents and is the representative ticket. There were a total of 92 Mishandling incidents this reporting period. Because of repetition, the other 91 are not included in this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered where appropriate.

Security Privacy Event Number: PSETS0000145520

DBCT Category: CMOP Mismailed

Organization: VHA CMOP
Charleston, SC

Date Opened: 11/1/2016

Date Closed: 11/4/2016

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 Charleston VA Medical Center (534) 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 will be counseled and retrained in proper packing procedures.

Incident Update

11/01/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that Patient B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

On 11/1/2016, the CMOP employee was counseled and retrained in proper packing procedures.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for Mismailed CMOP incidents and is the representative ticket. There were a total of nine Mismailed CMOP incidents out of 6,658,803 total packages (9,720,890 total prescriptions) mailed out for this reporting period. Because of repetition, the other eight are not included in this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Event Number: PSETS0000145595

DBCT Category: Mismailed

Organization: VISN 22
Loma Linda, CA

Date Opened: 11/2/2016

Date Closed: 11/15/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

The Privacy Officer received a call today from Veteran A. Veteran A received an evaluation letter. Along with Veteran A's evaluation letter was another evaluation letter for Veteran B.

Incident Update

11/01/16:
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 HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

The employee responsible for the mismailing will retake privacy awareness training. The Privacy Officer spoke with Veteran A and he will mail back the letter belonging to Veteran B. HIPAA notification letter has been sent out to Veteran B. The letter has been returned to the VA.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for Mismailed incidents and is the representative ticket. There were a total of 107 Mismailed incidents this reporting period. Because of repetition, the other 106 are not included in this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered where appropriate.

Security Privacy Event Number: PSETS0000146319

DBCT Category: Mishandling

Organization: VISN 15
St Louis, MO

Date Opened: 11/18/2016

Date Closed:

Date of Initial DBCT Review: 11/22/2016

No. of Credit Monitoring: 88

No. of Loss Notifications:

Incident Summary

Medical Student had patient lists in lab coat pocket. She left her coat in her car. Her car was broken into and the coat and lists were stolen.

Incident Update

11/21/16:
A lead analyst at VISN 15 will be running reports tomorrow to attempt to identify which Veterans and how many names were on the lists.

11/29/16:
The PO has an estimate of 30 patients involved. The student is not on rotation at the VA anymore. DBRS staff has asked the PO to get with the school program coordinator to get answers if the student will not respond to questions.

12/02/16:
Reports have been run with the names of the two attendings and three residents she worked with during the student's three weeks at the medical center. The lists would have contained a maximum of 88 Veterans. After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 88 Veterans will be sent letters offering credit protection services.

DBCT Decision Date: 12/06/2016

DBCT

DBCT concurred this was a data breach and credit protection services should be offered.

Security Privacy Event Number: PSETS0000146553

DBCT Category: IT Equipment Inventory

Organization: VISN 11
Indianapolis, IN

Date Opened: 11/28/2016

Date Closed: 11/29/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

During a Service laptop inventory, two VA laptops were discovered missing and reported to the ISO, Logistics and Police Service as lost. The VA laptops did have encrypted hard drives and were password protected with strong passwords. The laptops were assigned to rotating clinical staff.

Incident Update

11/28/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, Â§ C (Risk Assessment), Paragraph 1 (d), the Data Breach Response Service has determined that no breach has occurred. The laptops were encrypted. Therefore, this incident has a low probability of a risk of compromise due to the risk having been properly mitigated through established controls.

Resolution

The VA Service has updated their process for issuing/inventory VA laptops, to include the following:

1. Laptops that are not in use will be stored in a locked office, inside a locked cabinet.
2. A sign out/in sheet will be used to track laptops, while a solution to use PIV cards with the laptop security cabinet, is implemented.
3. Users will be issued cable locks to be used to secure the laptops, while in locked team rooms.
4. Laptops will be returned/inventoried after each Resident/Trainee rotation

DBCT Decision Date

DBCT

No DBCT decision was required. This is informational for IT Equipment Inventory incidents and is the representative event. There were two IT Equipment Inventory Incidents this reporting period. Because of repetition, the other incident is not included in this report.

Page left blank.

DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Data Breach Response Service

Monthly Report to Congress of Data Incidents

December 1 - 31, 2016

Security Privacy Ticket Number: PSETS0000146714

DBCT Category: Mishandling

Organization: VBA
St Louis, MO

Date Opened: 12/1/2016

Date Closed: 12/20/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring: 1

No. of Loss Notifications:

Incident Summary

Veteran A requested his records and when he received them it also contained records of Veteran B.

Incident Update

12/08/16:
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 letter offering credit protection services.

Resolution

The employees involved have been counseled.

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 80 Mis-Handling incidents this reporting period. Because of repetition, the other 79 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:	PSETS0000146743
DBCT Category:	Mismailed
Organization:	VISN 20 Portland, OR
Date Opened:	12/1/2016
Date Closed:	1/10/2017
Date of Initial DBCT Review:	12/6/2016
No. of Credit Monitoring:	
No. of Loss Notifications:	162

Incident Summary

A Veteran received an appointment letter from the facility and folded with the letter in the envelope were four pages of a patient list with information on 162 unique Veterans. The list contained last name, first initial, last four of the SSN, a clinic appointment title and the date of that appointment. The Veteran who received the list contacted and mailed the documents to the facility Privacy Officer. The documents were out of VA control for approximately two weeks.

Incident Update

12/06/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 162 Veterans will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

12/30/16:
Per an update from the Privacy Officer, there is one Veteran who is deceased. The new total is 161 Veterans who will be sent HIPAA notification letters, and the Next of Kin of the deceased Veteran will receive a Next of Kin notification.

Resolution

The office that mistakenly mailed the patient list is modifying their office procedures to have staff double check outgoing mail for content.

DBCT Decision Date: 12/06/2016

DBCT

12/06/16:
The DBCT concurred with the breach recommendation and determined that 162 affected individuals would be sent a HIPAA notification.

Security Privacy Ticket Number:	PSETS0000146869
DBCT Category:	CMOP Mismailed
Organization:	VHA CMOP Hines, IL
Date Opened:	12/2/2016
Date Closed:	12/9/2016
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 VA 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

12/02/16:
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 12/2/2016, 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 3 Mis-Mailed CMOP incidents out of 6,822,594 total packages (9,947,665 total prescriptions) mailed out for this reporting period. Because of repetition, the other 2 are not included in this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number: PSETS0000147332

DBCT Category: Mismailed

Organization: VISN 20
Seattle, WA

Date Opened: 12/8/2016

Date Closed: 12/9/2016

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

Veteran A received mailed prescription belonging to Veteran B. Veteran A contacted the pharmacy, returned the prescription, both Veteran A & B then received correct medications.

Incident Update

12/08/16:
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

Applicable employee was counseled concerning responsibilities when mailing medication.

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 134 Mis-Mailed incidents this reporting period. Because of repetition, the other 133 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: PSETS0000147426

DBCT Category: Mishandling

Organization: VISN 10
Columbus, OH

Date Opened: 12/12/2016

Date Closed:

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 179

Incident Summary

A VA employee emailed PII externally that contained information on VA patients to three different applicants by mistake.

Incident Update

12/15/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 178 Veterans will be sent a notification letter, in addition, one Next of Kin notification will be sent.

Resolution

The three applicants were contacted and notified to delete the emails. The individual who sent the email was counseled to pay more attention to what they are sending.

DBCT Decision Date:

DBCT

12/20/16:
The DBCT concurred with the breach recommendation and determined that the affected individuals would be sent a HIPAA notification.

Security Privacy Ticket Number:	PSETS0000147622
DBCT Category:	Mishandling
Organization:	VISN 16 Muskogee, OK
Date Opened:	12/15/2016
Date Closed:	12/29/2016
Date of Initial DBCT Review:	N/A
No. of Credit Monitoring:	93
No. of Loss Notifications:	

Incident Summary

On 12/15/16 at approximately 11:30 AM, a Veteran notified VA staff, that there was something on the ground in front of the dumpster that he believed should not be there and reported a possible violation. Police and a nurse from one of the teams went out and removed the contents of blood vials lying on the ground filled with blood and information for each patient of which the blood was drawn. On the vial labels it contained the full name and full social security number. The vial rack actually contained 93 Veteran specimens, 30 of which were recovered with 63 unaccounted for.

Incident Update

12/20/16:
At this point, 30 of the vials were unattended in a public parking area overnight. The other 63 are believed to be in the city dump, but this cannot be verified. There is no proof that a breach did not occur, therefore after review and analysis, in accordance with VA Handbook 6500.2, Section 5, and the Data Breach Response Service has determined that 93 Veterans will be sent letters offering credit protection services.

Resolution

Upon further investigation, it was discovered that an employee went to the trash bin and noticed the vials on the ground but did not pick them up due to the fact it was dark and the employee did not have on glasses to determine what it was, so he passed by them. The employee also noticed that there was a white bag which was torn on the ground. Upon completing this investigation it has been determined that lab specimens were misplaced in a clear bag and then transferred out to in a white trash bin as a normal procedure by housekeeping. The bag somehow got ripped during the night while the trash was being dumped by the city trash truck. The Privacy Officer (PO) will recommend additional training to staff and a process will be implemented to assure that lab specimen are all placed in the correct color bags labeled RED and disposed of properly.

DBCT Decision Date:

DBCT

12/20/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Core Team concurred with the DBRS recommendation that 93 Veterans will be sent letters offering credit protection services.

Security Privacy Ticket Number: PSETS0000148024

DBCT Category: IT Equipment Inventory

Organization: VISN 10
Dayton, OH

Date Opened: 12/23/2016

Date Closed:

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

Staff is unable to locate an encrypted PC during equipment inventory.

Incident Update

12/23/16:
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 Workstation was 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 56 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 55 are not included in this report.

Page left blank.