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

Monthly Report to Congress of Data Incidents

January 1 - 31, 2017

Security Privacy Ticket Number:	PSETS0000148309
DBCT Category:	Mishandling
Organization:	VISN 01 Providence, RI
Date Opened:	1/3/2017
Date Closed:	1/9/2017
Date of Initial DBCT Review:	N/A
No. of Credit Monitoring:	1
No. of Loss Notifications:	

Incident Summary

A provider handed the wrong appointment slip to Veteran A. When he got home he realized it was Veteran B's document. The document included Veteran B's name, full SSN, and medical information. Veteran A shredded the documents.

Incident Update

01/03/17:
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 was verbally counseled on being more vigilant when printing and handing out patient appointment information.

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 83 Mis-Handling incidents this reporting period. Because of repetition, the other 82 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: PSETS0000148315

DBCT Category: Mismailed

Organization: VBA
Des Moines, IA

Date Opened: 1/3/2017

Date Closed: 1/17/2017

Date of Initial DBCT Review: N/A

No. of Credit Monitoring: 1

No. of Loss Notifications:

Incident Summary

Veteran A received a letter which contained Veteran B's information, including his name, full SSN, medical information, and address.

Incident Update

01/03/17:
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 supervisor provided training and awareness to the employees that caused the violation.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for Mis-Mailed incidents and is the representative ticket. There were a total of 161 Mis-Mailed incidents this reporting period. Because of repetition, the other 160 are not included in this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Security Privacy Ticket Number: PSETS0000148319

DBCT Category: CMOP Mismailed

Organization: VHA CMOP
Dallas, TX

Date Opened: 1/3/2017

Date Closed: 1/9/2017

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 were compromised. Patient A reported the incident to the South Texas Veterans HCS 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

01/03/17:
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

Due to a unique repacking situation that occurred, we cannot conclusively validate which packer committed this error. On 01/06/17, all packers where made aware of this incident and current packing procedures where reviewed with packing staff.

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 seven Mis-Mailed CMOP incidents out of 6,897,591 total packages (10,133,755 total prescriptions) mailed out for this reporting period. Because of repetition, the other six are not included in this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number: PSETS0000148341

DBCT Category: IT Equipment Inventory

Organization: VISN 17
Harlingen, TX

Date Opened: 1/3/2017

Date Closed:

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

One VA-owned laptop and one VA-owned tablet were unable to be located during the annual IT inventory. They were last identified as being located in key restricted areas.

Incident Update

01/04/17:
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 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

Both devices were encrypted.

DBCT Decision Date:

DBCT

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.

Security Privacy Ticket Number:	PSETS0000148767
DBCT Category:	Mismailed
Organization:	VISN 09 Memphis, TN
Date Opened:	1/9/2017
Date Closed:	
Date of Initial DBCT Review:	1/10/2017
No. of Credit Monitoring:	
No. of Loss Notifications:	687

Incident Summary

A Principal Investigator (PI) contacted the PO and ISO regarding the mailing of 961 research study survey letters mailed with the wrong names on the letters. The PO was informed that the mailing address was correct; however, the wrong study subject's name from another group (same research study) was placed on the letters.

The Privacy Officer was informed by the PI that the survey letters mailed had the wrong names on the letters were accidently entered on the correct mailing intended for another group within the same research study. The PI has received several calls about the wrong names on the mailings with the correct mailing address for one of the Groups. The survey letter did not contain any SSNs, only the survey questions about pain medication taken by the research subject.

Incident Update

01/10/16:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, and consultation with DBCT it was determined that 961 Veterans will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

01/24/17:
The Privacy Officer reports that 240 letters were returned undeliverable, so the new count is 720 affected Veterans will get letters.

02/07/17:
The Privacy Officer reports that after duplicates have been removed the final count of Veterans involved is 687.

02/15/17:
The letters were processed and mailed on 02/14/17.

DBCT Decision Date: 02/24/2017

DBCT

The DBCT concurred that this was a data breach and credit monitoring will be required.

Security Privacy Ticket Number:	PSETS0000148824
DBCT Category:	Mishandling
Organization:	VISN 20 Seattle, WA
Date Opened:	1/10/2017
Date Closed:	
Date of Initial DBCT Review:	1/17/2017
No. of Credit Monitoring:	36
No. of Loss Notifications:	337

Incident Summary

Everett Transit Authority (ETA) needed to speak to someone in the Research Department as they had "found an item". The message was passed on through several hands before reaching someone who able to call the ETA back and found out, on Wednesday 01/04/17, that this was a USB flash drive that appeared to be associated with a principal research investigator (PI) at Puget Sound (PUG).

Upon learning this, research staff drove to Everett and picked up the flash drive and brought it back. It was secured in the research office per direction of the Admin Officer for Research. The drive was locked up but not looked at until 01/06/17 (for various reasons). Whereupon it was noted that a) the drive is unencrypted and had both personal and research data on it, b) the drive contains a fair amount of copied data on older studies of the PI, and c) at least one or two folders contain name, street and/or email address of subjects (aka PHI).

For background context, most of the data files are from 2004 to 2009. In the early to mid-2000s, VA did not provide encrypted flash drives and the research department did not have their own dedicated storage server, as they do now. Many studies at that time stored copies of the research data on drives purchased by research as a way to work on data at multiple locations and provide a backup (again, no dedicated research server and not enough storage space on the "regular" servers in many instances).

It would appear this is one of those drives. The research group thought they had collected and properly stored all such drives prior to this loss. This researcher may have just forgotten that this drive had research data on it, as it also contains some of her personal data, and since it was not labeled as belonging to VA.

Upon review, it was determined this drive belonged to a research staff member who had left service in May, 2016. The PI contacted this researcher and discussed this with her. They came to the tentative conclusion that the drive was most likely lost because this researcher had packed up some of her items to be shipped to her new location and left them with a friend in a box to be shipped. The person was supposed to mail this box to the researcher but does not appear to have done so yet.

An ETA employee plugged the drive in and was able to find many folders labeled with the name of the PI and thus able to trace to the PUG VA hospital. VA staff are currently reviewing the over 500 files on the drive to collect the number of subjects/Veterans affected and what data was included. We will report that information as soon as we have it.

Incident Update

01/17/17:
The Data Breach Core Team has determined that this incident is a data breach and will require HIPAA notification letters and letters offering credit protection services where warranted.

In accordance with VA Handbook 6500.2, Section 5, the Data Breach Core Team has determined that 36 individuals will be sent letters offering credit protection services due to full name and SSN being disclosed. An additional 373 individuals will be receiving HIPAA notification letters due to Protected Health Information being disclosed.

DBCT Decision Date: 01/17/2017

DBCT

The Data Breach Core Team has determined that this incident is a data breach and will require HIPAA notification letters and letters offering credit protection services where warranted.

Security Privacy Ticket Number:	PSETS0000149320
DBCT Category:	Mishandling
Organization:	VISN 15 St Louis, MO
Date Opened:	1/17/2017
Date Closed:	
Date of Initial DBCT Review:	1/31/2017
No. of Credit Monitoring:	48
No. of Loss Notifications:	676

Incident Summary

The Privacy Officer received an email from a VA Attorney at OGC stating that she is representing VA in an EEO case regarding a former St. Louis VA employee. The attorney recently received documents in the mail in response to a discovery request that contained VistA print outs of scheduled consults that had Veterans' last name, first initial, and last 4 SSN of "many Veterans" some including those that received HIV counseling. The Privacy Officer has requested copies of the documents to be able to review them for content.

Incident Update

01/24/17:
The attorney asked the two AFGE union representatives who are "representing" the former employee where these records came from and they told her that the former employee gave them to the AFGE representatives to send to her. The former employee had the records in his possession. He has been separated from employment since January, 2016.

The Privacy Officer is meeting with one of the AFGE representatives on 01/24/17, and will attempt to determine how the records came to be in the ex-employee's possession and how the records were stored between the time he obtained them until the time they were given to the AFGE and the attorney.

01/31/17:
The Data Breach Core Team determined this incident to be a data breach. The number of affected individuals is 724. The breakdown of notification letters and offers of credit protection services are as follows:
HIPAA Notifications: 615
Credit Protection Services: 48
Next of Kin Notifications: 61

This incident is HITECH 500+ reportable and requires a press release.

The Privacy Officer is on track to have the letters in the mail no later than 02/24/17.

DBCT Decision Date: 01/31/2017

DBCT

The Data Breach Core Team determined that this incident is a data breach and will require notifications and credit protection services where warranted.

Page left blank.

DEPARTMENT OF VETERANS AFFAIRS
Data Breach Response Service

Monthly Report to Congress of Data Incidents

February 1 - 28, 2017

Security Privacy Event Number: PSETS0000150175

DBCT Category: Mismailed

Organization: VBA
Winston-Salem, NC

Date Opened: 2/1/2017

Date Closed: 2/8/2017

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 the mail.

Incident Update

02/01/17:
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 Privacy Officer contacted Veteran B whose personal information was compromised and sent a letter offering credit protection services. The PO then contacted Veteran A and retrieved Veteran B's notification letter. The PO contacted the VA employee who created the incorrect letter and required the employee to complete Privacy Awareness training.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for mismailed incidents and is the representative event. There were a total of 157 mismailed incidents this reporting period. Because of repetition, the other 156 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 Event Number: PSETS0000150232

DBCT Category: Mishandling

Organization: VISN 20
Roseburg, OR

Date Opened: 2/1/2017

Date Closed: 2/9/2017

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

Veteran A was added to Veteran B's progress note. The note was released to Veteran B. Veteran B was contacted and returned the note. Veteran B was provided a copy of the corrected note.

Incident Update

02/02/17:
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 HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

The employee was given additional privacy training on February 1, 2017. A notification letter was mailed to the Veteran explaining the accidental disclosure.

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for mishandled incidents and is the representative event. There were a total of 77 mishandled incidents this reporting period. Because of repetition, the other 76 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 Event Number:	PSETS0000150956
DBCT Category:	CMOP Mismailed
Organization:	VHA CMOP Hines, IL
Date Opened:	2/16/2017
Date Closed:	2/27/2017
Date of Initial DBCT Review:	N/A
No. of Credit Monitoring:	
No. of Loss Notifications:	1

Incident Summary

Patient A received a prescription paperwork intended for Patient B. Patient B's name and medication type was compromised. Patient A reported the incident to the VA medical center and the patient has been instructed to destroy or return the paperwork by the VA Medical Center. 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

02/16/17:
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 2/16/2017, T]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 event. There were a total of seven mismailed CMOP incidents out of 5,958,811 total packages (8,844,318 total prescriptions) mailed out for this reporting period. Because of repetition, the other six are not included in this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Event Number: PSETS0000151012

DBCT Category: Mishandling

Organization: VISN 16
Fayetteville, AR

Date Opened: 2/17/2017

Date Closed:

Date of Initial DBCT Review: 2/28/2017

No. of Credit Monitoring: 61

No. of Loss Notifications:

Incident Summary

An employee contacted Environmental Services to pick up sensitive confidential shred. The shred was never picked up, and staff left for the day leaving the sensitive shred bag in the copy room. The next morning, staff noticed the bag was gone and was concerned that the cleaning crew may have picked it up. The staff contacted Environmental Services and received confirmation that the shred bag was not picked up by them. The sensitive shred was picked up by the cleaning staff and disposed with the regular trash. The City of Fayetteville was contacted, and confirmation was given that the trash was picked up early this morning and taken to the landfill.

Incident Update

03/07/17:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 61 Veterans will be sent letters offering credit protection services.

DBCT Decision Date: 03/07/2017

DBCT

The Data Breach Core Team (DBCT) has concurred that 61 Veterans will be sent letters offering credit protection services.

Security Privacy Event Number: PSETS0000151256

DBCT Category: IT Equipment Inventory

Organization: VISN 23
Iowa City, IA

Date Opened: 2/23/2017

Date Closed: 3/7/2017

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 one (1) encrypted laptop could not be located.

Incident Update

02/24/17:
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 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.

Resolution

The device hard drive was encrypted; any data on the device is inaccessible.

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

Security Privacy Event Number:	PSETS0000151498
DBCT Category:	Mishandling
Organization:	VISN 08 West Palm Beach, FL
Date Opened:	2/27/2017
Date Closed:	3/14/2017
Date of Initial DBCT Review:	3/7/2017
No. of Credit Monitoring:	7
No. of Loss Notifications:	62

Incident Summary

A Paralegal Specialist found a folder on Women's Bathroom on 3C. The folder contained many handwritten documents from Veterans. The Information Security Officer (ISO) and the Privacy Officer (PO) made an overview and determined that at least 6 full SSNs were found along with Veteran's Full Name, DOB; and 282 partial SSN were found along with Veteran's full name, room bed, admission dates and diagnosis. Also identified were at least 6 Veterans with 7332 information. The majority of the documents were signed by a Mental Health Provider.

Incident Update

03/02/17:
After removing duplicates, the information found belongs to 69 unique Veterans. PO has determined that the full SSN was disclosed for seven Veterans, including their full DOB, diagnosis, medications, admissions date and room number. In addition, partial SSN was disclosed from 62 Veterans along with diagnosis, medications, admissions dates and room number. From the 69 Veterans, there were 17 diagnosis protected by the USC 7332 statute.
The employee who left the documents has been identified; however, it is not known how long the documents were left in the restroom. The restroom is in an inpatient mental health ward and accessible to other patients and visitors. After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that seven Veterans will be sent a letter offering credit protection services. A HIPAA notification letter will be sent to 62 Veterans.

Resolution

Notification was provided to employee's supervisor for immediate action. Training was provided immediately to employee and all Mental Health Providers. Credit Monitoring Letters and HIPAA Notifications were sent to Veterans affected.

Security Privacy Event Number: PSETS0000151498 (continued)

DBCT Decision Date: 03/07/2017

DBCT

The Data Breach Core Team (DBCT) has concurred that 69 Veterans would receive letters offering credit protection services and/or HIPAA notification letters where 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

March 1 - 31, 2017

Security Privacy Ticket Number:	PSETS0000151577
DBCT Category:	Mishandling
Organization:	VISN 19 Denver, CO
Date Opened:	3/1/2017
Date Closed:	3/15/2017
Date of Initial DBCT Review:	N/A
No. of Credit Monitoring:	68
No. of Loss Notifications:	1

Incident Summary

An employee left lab tissue on a cart outside the freight elevators for an estimated 24 hours because he/she could not get into the morgue. The elevators are accessible by everyone.

Incident Update

03/07/17:

The area the elevators are not a "staff only" area and is traveled by employees, Veterans/patients as well as visitors. The lab specimens were "Anatomic Pathology Specimens". Upon further review, the PO indicates that in addition to full name, full SSN, the full date of birth is also on the labels. After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 76 Veterans will be sent letters offering credit protection services.

03/09/17:

Update: One Veteran is deceased; therefore the next of kin for that Veteran will receive a notification letter. Additionally, some duplicates were discovered, the updated total is now: 68 Veterans will receive credit protection services and one Next of Kin notification will be sent.

Resolution

Administrative Action has been recommended and forwarded to the supervisor and HR.

DBCT Decision Date:

DBCT

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

Security Privacy Ticket Number:	PSETS0000151579
DBCT Category:	Mismailed
Organization:	VBA Phoenix, AZ
Date Opened:	3/1/2017
Date Closed:	3/2/2017
Date of Initial DBCT Review:	N/A
No. of Credit Monitoring:	1
No. of Loss Notifications:	

Incident Summary

Veteran A requested copy of his DD 214, from the NCC. He received another Veteran B's DD 214, containing Veteran B's military service information to included full name and SSN. Veteran A, will mail DD 214 back to Phoenix RO.

Incident Update

03/01/17:
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

NCCM was notified so she can provide counseling to individual who sent DD 214.

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 200 Mis-Mailed incidents this reporting period. Because of repetition, the other 199 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 Ticket Number:	PSETS0000151603
DBCT Category:	Mishandling
Organization:	VISN 10 Dayton, OH
Date Opened:	3/1/2017
Date Closed:	
Date of Initial DBCT Review:	4/4/2017
No. of Credit Monitoring:	223
No. of Loss Notifications:	

Incident Summary

Employee A's name was found on three fellow employees SPAR Reports. The employee has no reason to access the fellow employee's medical records.

Incident Update

03/02/17:
PO update -- Supervision confronted employee regarding inappropriate access to fellow employee's medical records. Employee resigned today and has agreed to provide a report of contact by COB 3-6-2017. Affected employees have all provided reports of contact to supervision.

03/06/17:
PO update -- One employee whose name is found on the report is requesting credit monitoring.

03/07/17:
PO update -- Employee who accessed the records resigned from this facility March 2, 2017

03/09/17:
PO update -- Fact finding investigation ongoing,

03/16/17:
PO update -- Fact Finding continues in the home service.

03/21/17:
PO update -- Following up on the internal investigation provided to the PO from the Service.

03/24/17:
PO update -- Still interpreting the fact finding results.

04/03/17:
PO update -- PO changed complaint to an incident - It has been determined that the ex-employee accessed 223 Veteran and employee electronic medical records. There is no apparent explanation why he should have accessed this large number of records. Fact finding substantiates that this individual shared information regarding the three (2 employees and 1 patient) with other VA employee staff.

04/10/17:
PO update -- From the list of CPRS accesses via the Sensitive Patient Access Report that was provided to us, the following data was pulled:

1 volunteer
3 current employees (fellow employees in the offenders department)
1 deceased employee (died in February)
3 former employees (unknown at this time how long ago they were employees)

The rest are patients
It is difficult for us to know what was authorized or not. There were some accesses that were close to appointment times

253 total access (some were multiple access on the same individual)
91 had an associated appointment around the time of the access
155 had no associated appointments
7 on the list were unable to associate with appointments

The facility is only aware of him discussing three individual with the other employees.

04/11/17:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 223 Veterans/Patient/Employee will be sent letters offering credit protection services.

DBCT Decision Date: 04/11/2017

DBCT
4/11/17:
The DBCT met on 4/11/17 and agreed that this was a data breach and that all parties should receive letters offering credit protection services.

Security Privacy Ticket Number: PSETS0000151607

DBCT Category: IT Equipment Inventory

Organization: VISN 23
Iowa City, IA

Date Opened: 3/1/2017

Date Closed: 3/7/2017

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

During routine VA Logistics equipment inventory it was found that one encrypted Smart Phone was reported lost.

Incident Update

03/01/17:
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 Smart Device or Tablet was encrypted and per policy will be disabled. Therefore this incident has a low probability of a risk of compromise due to the risk having been properly mitigated through established controls.

Resolution

In June of 2016 the cellular phone was deactivated, unable to be recovered after a motor vehicle accident. The device was encrypted; any data on the device is inaccessible

DBCT Decision Date:

DBCT

No DBCT decision is required. This is informational for IT Equipment Inventory incidents and is the representative ticket. There were a total of 3 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 2 are is not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Security Privacy Ticket Number: PSETS0000151700

DBCT Category: Mishandling

Organization: VISN 01
Manchester, NH

Date Opened: 3/3/2017

Date Closed: 3/28/2017

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 1

Incident Summary

Privacy Officer received a call from the Provider who made the mistake and handing the wrong appointment list to the wrong Veteran (Veteran A received Veteran B's list). This list was returned by the Veteran/Ex-employee, who then retrieved the correct appointment list. The Veteran's Social Security number was black out.

Incident Update

03/03/17:
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

Education was given and the document was retrieved. An action plan was put in place.

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 88 Mis-Handling incidents this reporting period. Because of repetition, the other 84 are not included in this report, but are included in the "Mis-Handling 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 Ticket Number:	PSETS0000152397
DBCT Category:	Mishandling
Organization:	VACO Field Program Office Murfreesboro, TN
Date Opened:	3/17/2017
Date Closed:	
Date of Initial DBCT Review:	3/21/2017
No. of Credit Monitoring:	113
No. of Loss Notifications:	

Incident Summary

Employee teleworking 100% due to RA. Trained and gave access to boyfriend and he has been accessing Veteran accounts daily; completing her workload for her.

Incident Update

04/03/17:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Core Team has confirmed that 113 Veterans will be sent letters offering credit protection services.

Resolution

Employee has turned in Government owned laptop, VPN account has been disabled and all account accesses have been terminated. Department Manager is working with ER/LR for additional disciplinary action. Credit letter has been mailed to all Veterans affected by this security breach (attached).

DBCT Decision Date: 04/04/2017

DBCT

04/03/17:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Core Team has confirmed that 113 Veterans will be sent letters offering credit protection services.

Security Privacy Ticket Number:	PSETS0000152502
DBCT Category:	CMOP Mismailed
Organization:	VHA CMOP Murfreesboro, TN
Date Opened:	3/20/2017
Date Closed:	3/21/2017
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. Murfreesboro 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

03/20/17:
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 3/20/2017, 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 13 Mis-Mailed CMOP incidents out of 7,166,719 total packages (10,651,877 total prescriptions) mailed out for this reporting period. Because of repetition, the other 12 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 Ticket Number: PSETS0000152514

DBCT Category: Missing/Stolen Equipment (Other)

Organization: VISN 20
Anchorage, AK

Date Opened: 3/20/2017

Date Closed: 4/4/2017

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications:

Incident Summary

Approximately 10:30 am a VA Employee entered the warehouse at the Northway Mall VA office area, and discovered there was a physical breach of the back door. Further investigation found that a number of brand new computers and monitors were missing. At 11:31 FCIO informed the ISO that the warehouse had been breached and approximately 9 computers, 6 monitors, and 2 - 65" monitors are missing. The verified computers that are missing are new and have not been imaged yet, there are currently no computers with information on them missing. VA Police, IT, and Facilities personnel are currently at the Northway Facility to establish the exact count and extent of the break-in.

Incident Update

03/21/17:
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 new equipment had never been imagined and as no VA Data on them.

Resolution

Incident Report filed with the VA OIG. The new equipment had never been imagined and as no VA Data on them. Facility is currently reviewing its storage facilities to prevent thefts in the future.

DBCT Decision Date:

DBCT

No DBCT decision needed. This stays on as informational for missing equipment.

page left blank

DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Incident Resolution Service

Monthly Report to Congress of Data Incidents
April 1 - 30, 2017

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000153169	Mishandled/ Misused Physical or Verbal Information	VBA St Petersburg, FL	4/3/2017	4/4/2017	

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number/Category	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	N/A	N/A	N/A	N/A	N/A		1

Incident Summary

Veteran A received a letter intended for Veteran B

Incident Update

04/03/17:
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

The employees were given additional training and best practices in proper safe guarding of documents.

DBCT

DBCT Decision Date: N/A

No DBCT decision is required. This is informational for Mis-Mailed incidents and is the representative ticket. There were a total of 155 Mis-Mailed incidents this reporting period. Because of repetition, the other 154 are not included in this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000153196	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Charleston, SC	4/3/2017	4/10/2017	

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number/Category	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	N/A	N/A	N/A	N/A	N/A		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 Dorn 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 will be counseled and retrained in proper packing procedures.

Incident Update

04/03/17:
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 4/3/2017, the CMOP employee was counseled and retrained in proper packing procedures

DBCT

DBCT Decision Date: N/A

No DBCT decision is required. This is informational for Mis-Mailed CMOP incidents and is the representative ticket. There were a total of 15 Mis-Mailed CMOP incidents out of 6,234,069 total packages (9,249,691 total prescriptions) mailed out for this reporting period. Because of repetition, the other 14 are not included in this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000153200	Unauthorized Electronic Access	VISN 04 Philadelphia, PA	4/3/2017	4/24/2017	

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number/Category	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	N/A	N/A	N/A	N/A	N/A		1

Incident Summary

The spouse of an employee printed a copy of Veterans information and provided it to family court for her child support hearing.

Incident Update

04/03/17:
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 HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

Resolution

Disciplinary action is being taken towards the staff member.

DBCT

DBCT Decision Date: N/A

No DBCT decision is required. This is informational for Mis-Handling incidents and is the representative ticket. There were a total of 71 Mis-Handling incidents this reporting period. Because of repetition, the other 70 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	Incident Type	Organization	Date Opened	Date Closed	Date of Initial DBCT Review
PSETS0000153658	Mishandled/ Misused Physical or Verbal Information	VISN 21 Palo Alto, CA	4/11/2017		4/18/2017

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number/Category	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	N/A	N/A	N/A	N/A	N/A	76	1

Incident Summary

The Privacy Officers were notified by the VA Police that a report was filed for a missing binder with "return clinic appointments order" that contained information on approximately 50 Veterans. According to the reporter, the binder was placed in a locked cabinet on 4/7/17; it was noted missing 4/10/17.

Incident Update

04/17/17:
The missing list was re-created to determine the number of individuals affected, there were 77 Veterans information compromised. The list includes full names, full social security numbers, and personal phone numbers and clinic names. The reporting process has been converted electronically. A hard copy is no longer utilized.

After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 77 Veteran will be sent a letter offering credit protection services and one notification letter will be sent to the Veterans next of Kin.

Resolution

All 77 notification letter were sent to the Veterans affected on 5/3/17.

DBCT

DBCT Decision Date: N/A

No DBCT decision required. This incident was presented to the DBCT for awareness based on the numbers affected.

page left blank

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

Monthly Report to Congress of Data Incidents

May 1 - 31, 2017

Security Privacy Ticket Number:	PSETS0000154639
DBCT Category:	Mishandling
Organization:	VISN 20 Portland, OR
Date Opened:	5/1/2017
Date Closed:	
Date of Initial DBCT Review:	5/23/2017
No. of Credit Monitoring:	42
No. of Loss Notifications:	23

Incident Summary

An estate attorney called to report a deceased employee's house was being cleaned and boxes of VA medical records were found in her garage. It is unknown what the boxes contain. The facility is arranging secure pick up.

Incident Update

05/22/17:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that 42 Veterans will be sent letters offering credit protection services and 23 will receive a HIPPA notification letters.

DBCT Decision Date: 05/23/2017

DBCT

The Data Breach Core Team concurred that 42 Veterans will be sent letters offering credit protection services and 23 will receive a HIPPA notification letters.

Security Privacy Ticket Number:	PSETS0000155220
DBCT Category:	Mishandling
Organization:	VISN 16 Shreveport, LA
Date Opened:	5/8/2017
Date Closed:	5/10/2017
Date of Initial DBCT Review:	N/A
No. of Credit Monitoring:	1
No. of Loss Notifications:	

Incident Summary

A VA Nurse attached the wrong labs to Veteran A's package for clinician review. The doctor reviewed the labs belonging to Veteran A with Veteran B and subsequently released Veteran A's lab results to Veteran B in paper form. Later that evening, the doctor contacted Veteran B and requested return of the lab paperwork. All paperwork has been returned and the incident has been documented in Veteran B's medical record.

Incident Update

05/09/17:
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

All lab staff has been educated on the need to cross-check documentation prior to discussion and/or release.

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 111 Mis-Handling incidents this reporting period. Because of repetition, the other 110 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: PSETS0000155523

DBCT Category: CMOP Mismailed

Organization: VHA CMOP
Murfreesboro, TN

Date Opened: 5/12/2017

Date Closed: 5/22/2017

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, address and type of medication was compromised. Patient A reported the incident to the medical center and a replacement has been requested for Patient B. The Murfreesboro Consolidated Mail Outpatient Pharmacy (CMOP) investigation concluded that this was a CMOP packing error. The CMOP employee(s) will be counseled and retrained in proper packing procedures.

Incident Update

05/15/17:
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

The CMOP employee has been 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 seven Mis-Mailed CMOP incidents out of 7,012,047 total packages (10,430,011 total prescriptions) mailed out for this reporting period. Because of repetition, the other six are not included in this report. In all incidents, Veterans will receive a notification letter.

Security Privacy Ticket Number: PSETS0000155805

DBCT Category: Mismailed

Organization: VISN 06
Durham, NC

Date Opened: 5/18/2017

Date Closed: 5/23/2017

Date of Initial DBCT Review: N/A

No. of Credit Monitoring:

No. of Loss Notifications: 2

Incident Summary

Veteran A alerted her primary care physician (PSP) that when she received her recent lab results in the mail, she also received echocardiogram results intended for Veteran B and tele-retinal results intended for Veteran C. Thus, two full names, partial SSN's, addresses, and medical information were disclosed in error.

Incident Update

05/18/17:
After review and analysis, in accordance with VA Handbook 6500.2, Section 5, the Data Breach Response Service has determined that Veterans B and C will be sent HIPAA notification letters due to Protected Health Information (PHI) being disclosed.

Resolution

This matter was referred to clinic leadership for administrative action as appropriate. Clinic staff has been reminded to review all documents and Veteran identities prior to mailing information.

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 199 Mis-Mailed incidents this reporting period. Because of repetition, the other 197 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.